Systemwalker Operation Manager Enterprise Edition V13.2.0 Windows版 セキュリティターゲット

Version 1.11

2007/12/18

富士通株式会社

FUJITSU

- 更新履歴 -

バージョン	日付	更新箇所	更新内容	作成者
1.00	2007/2/7	新規作成	—	富士通株式会社
1.01	2007/04/12	1～8 章	・誤記修正	富士通株式会社
1.02	2007/07/02	1～8 章	・記述の見直し	富士通株式会社
1.03	2007/07/20	1～8 章	・記述の見直し	富士通株式会社
1.04	2007/09/04	2～8 章	・記述の見直し	富士通株式会社
1.05	2007/10/12	1～8 章	・記述の見直し	富士通株式会社
1.06	2007/10/25	8 章	・記述の見直し	富士通株式会社
1.07	2007/10/31	2,6,8 章	・記述の見直し	富士通株式会社
1.08	2007/11/15	1～8 章	・記述の見直し	富士通株式会社
1.09	2007/11/28	1,4,8 章	・記述の見直し	富士通株式会社
1.10	2007/12/14	2 章	・記述の見直し	富士通株式会社
1.11	2007/12/18	2 章	・記述の見直し	富士通株式会社

- 目次 -

1 ST概説

本章では、ST 識別、ST 概要、CC 適合、参考資料、及び表記規則、用語、略語について記述する。

1.1 ST識別

1.1.1 STの識別

名称　　：Systemwalker Operation Manager Enterprise Edition V13.2.0
　　Windows 版　セキュリティターゲット
バージョン：Version 1.11
作成日　　：2007 年 12 月 18 日
作成者　　：富士通株式会社

1.1.2 TOEの識別

名称　　：Systemwalker Operation Manager Enterprise Edition
バージョン：V13.2.0　(Windows)
なお、TOE は、それぞれ、以下のクライアント、サーバのソフトウェアで構成される。
・クライアント
Windows 版 Systemwalker Operation Manager V13.2.0(Build-20070507) クライアント
・サーバ
Windows 版　Systemwalker Operation Manager Enterprise Edition　V13.2.0 (Build-20070507) サーバ

作成者　　：富士通株式会社

1.1.3 適用するCCのバージョン

- ISO/IEC 15408:2005
- 補足-0512 適用

1.2 ST概要

本 ST は、業務システムの自動運転を支援するソフトウェア製品である「Systemwalker Operation Manager Enterprise Edition」のセキュリティ仕様を規定している。

本 IT 製品を使用することにより、利用者は内部ネットワーク上に分散するサーバの起動・停止や、利用者の業務を、日々計画されたとおりに実行させるための運用管理を行い、多様化／複雑化している業務システムの運用管理をセキュアに行うことが可能となる。

本 IT 製品では、保護すべき資産として、上記の日々計画されたとおりにジョブを実行させる処理である「ジョブの計画的な実行」、及びそれに関連する資源を保護資産としている。これら保護資産への不正な行為に対して、以下のセキュリティ機能を提供する。

・利用者毎に操作できる範囲を制限する「アクセス制御機能」
・利用者の操作を検証するための「監査ログ出力機能」
・内部ネットワーク上に流れるパスワードを保護する「パスワード保護機能」

1.3 CC適合

本 ST は、以下を満たしている。

パート 2 適合
パート 3 適合
EAL 1 適合
適合する PP は存在しない。

1.4 参考資料

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model August Version 2.3 CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements August 2005 Version 2.3 CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements August 2005 Version 2.3 CCMB-2005-08-003
- Common Methodology for Information Technology Security Evaluation Evaluation Methodology August 2005 Version 2.3 CCMB-2005-08-004
- 情報技術セキュリティ評価のためのコモンクライテリア パート 1：
  概説と一般モデル 2005 年 8 月 バージョン 2.3 CCMB-2005-08-001 平成 17 年 12 月翻訳第 1.0 版 独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のためのコモンクライテリア パート 2：
  キュリティ機能要件 2005 年 8 月 バージョン 2.3 CCMB-2005-08-002 平成 17 年 12 月翻訳第 1.0 版
- 独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のためのコモンクライテリア パート 3：
  セキュリティ保証要件 2005 年 8 月 バージョン 2.3 CCMB-2005-08-003
  平成 17 年 12 月翻訳第 1.0 版 独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のための共通方法

評価方法 2005 年 8 月 バージョン 2.3 CCMB-2005-08-004
平成 17 年 12 月翻訳第 1.0 版 独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室

1.5 表記規則、用語、略語

1.5.1 表記規則

第 3 章の前提条件、脅威、組織のセキュリティ方針、及び第 4 章のセキュリティ対策方針では、それぞれのラベルを**ボールド体**フォントで記述し、続けてその定義を通常フォントで記述する。

1.5.2 用語、略語

本 ST で使用する用語、略語を定義する。

表 1-1 用語、略語の定義

用語、略語	定義内容
業務システム	本 TOE を導入し、運用管理を行う対象のシステムを示す。 業務システムは、スケジュールの管理を行うスケジュールサーバ、実際に利用者のプログラムが動作する業務サーバ、業務の運用管理を行う運用管理クライアントおよびそれらを相互接続するネットワークからなる。
自動運転	TOE を導入するシステムで動作する利用者のプログラム（以降、業務と記載）を自動実行する事を示す。
ジョブ	業務の自動実行を行う際の処理単位であり、特に、本 ST 内ではスケジュールされたジョブを指す。
リカバリジョブ	自動実行中のジョブが異常終了した場合に呼び出されるジョブであり、ジョブの異常終了で放置されている各種資源の復旧処理を行う。
ジョブネット	ジョブの集合である。
グループ	ジョブネットの集合である。
プロジェクト	グループの集合である。
JCL	ジョブの実行制御を行なう際に利用する言語。本言語により、複雑な業務の手順を容易に記述できる。OS ユーザにより作成される。ジョブを起動、終了する際に利用される。
バッチファイル	複数の処理をまとめて行なう際に使われるファイル
実行プログラム	ジョブを実行するプログラム。このプログラムにはコマンドが含まれる。

用語、略語	定義内容
自動運転用定義情報	ジョブの計画的な実行を行なう際に利用する定義情報である。 自動運転を行うための定義情報には、ジョブおよびリカバリジョブが登録される。
アクセス制御情報	アクセス制御機能の制御規則を規定した情報である。
監査ログファイル	セキュリティ機能に関する操作の記録したファイル
ジョブの実行記録	ジョブの実行に関わる記録である。
イベントログ	TOE が動作する OS にて採取するログである。
ポリシー情報	TOE の環境定義情報（管理対象のホストの情報）や登録情報（カレンダ機能に関する情報等）が定義されているデータ。 既に運用中のサーバから、本データを抽出して新規に導入するサーバに配付・適用することにより、すでに運用中のサーバと同じ運用環境を新規のサーバ上にも構築することができる。
OS ユーザ	コマンドを使用したシステム管理者、及び OS 一般ユーザを指す。
OMGR／MGR	Windows 版 Systemwalker Operation Manager Enterprise Edition V13.2.0 (Build-20070507) サーバの略称 Systemwalker Operation Manager Enterprise Edition のサーバ機能およびセキュリティ機能を提供するソフトウェアであり、スケジュールサーバおよび業務サーバ上で動作する。
OMGR／Client	Windows 版 Systemwalker Operation Manager V13.2.0 (Build-20070507) クライアントの略称 Systemwalker Operation Manager Enterprise Edition で運用管理を行うクライアント機能およびセキュリティ機能を提供するソフトウェアであり、管理クライアント上で動作する。 本 ST では、OMGR/MGR と連携して動作するクライアント機能およびセキュリティ機能を示す。
内部ネットワーク	TOE が動作する各サーバを LAN (IEEE802.3 インタフェース) 接続し、構築したネットワークセグメントである。 後述する外部ネットワークと異なり、企業内で構築されるイントラネットとして運用されるネットワークを示す。
外部ネットワーク	インターネットへの接続または、他企業と取引のため、相互接続を行っているネットワークセグメントである。
運用管理	ジョブの開始や終了といった運用に関わる行為
スケジューリング	ジョブの開始・終了時刻や、実行順序等を規定する行為
サーバ	本 ST においてサーバと示した場合、業務サーバ、スケジュールサーバを指す。

用語、略語	定義内容
運用管理業務	本 ST において、運用管理業務と記載した場合、以下の行為を指す。 ・自動運転用定義情報に対して、業務を行うためのジョブをスケジューリングする ・必要に応じて、ジョブスケジューラを使用して、ジョブ操作を行なう ・リカバリジョブを投入する ・ジョブの状態を確認する
ジョブの実行ユーザ	ジョブを登録する際に、ジョブの属性情報として設定することができる OS ユーザ。実行ユーザの権限でそのジョブは実行される。
ジョブ所有者情報の定義	ジョブの実行ユーザとして許可された OS ユーザが登録される定義ファイルである。
所有者	業務に対して、責任(「自動運転用定義情報」や「ジョブ」を所有する人物としての責任)を持つ OS 一般ユーザ。
ARCserve	BrightStor(R) ARCserve (R) Backup for Windows の略 バックアップ/リカバリを行なうサーバ。

2 TOE記述

本章では、TOE 種別、TOE 概要、TOE 構成、TOE の機能および保護対象となる資産について記述する。

2.1 TOE種別

本 TOE は業務システムの自動運転を支援するソフトウェア製品である。

2.2 TOE概要

2.2.1 TOEの利用目的

本 TOE は、業務サーバの起動や停止、ジョブの開始や終了といった日常の運用管理を、日々計画された通りに実行させる機能を持つソフトウェア製品である。

本 TOE において、業務システムの運用管理は、「自動運転用定義情報」と呼ばれる定義ファイルにてジョブおよびリカバリジョブのスケジュールを定義し、この定義ファイルに従い処理を実行することで実現する。

本 TOE では、この「自動運転用定義情報」に対する利用者のなりすましによる操作、許可されないアクセス、及び操作の前の識別認証に使用するパスワードの盗聴、に対処する機能を提供するため、利用者は業務システムの運用管理をセキュアに行うことが可能となる。

2.3 TOE構成

2.3.1 TOEの物理的構成

（１）TOE の物理的な構成要素

本 TOE の物理的構成要素は以下である。

- Windows 版 Systemwalker Operation Manager V13.2.0(Build-20070507)クライアント
  ※クライアントプログラムのこと。以降、OMGR/Client と表記

- Windows 版 Systemwalker Operation Manager Enterprise Edition V13.2.0 (Build-20070507) サーバ
  ※サーバプログラムのこと。以降、OMGR/MGR と表記

（２）TOE の動作環境

■TOE の動作に必要なハードウェア資源

OMGR/MGR及びOMGR/Clientの動作に必要なハードウェア資源を、表 2-1に示す。

表 2-1 TOE の動作に必要なハードウェア資源

	OMGR/MGR	OMGR/Client	
		Windows x64	Windows x64 以外
ディスク容量	79MB 以上	90MB 以上	90MB 以上
メモリ使用量	50MB 以上	50MB 以上	40MB 以上

また、LAN カードが必須である。

■ソフトウェア資源

OMGR/MGR及びOMGR/Clientの動作に必要なソフトウェア資源を、表 2-2に示す。

表 2-2 TOE の動作環境(ソフトウェア)

インストール種別	動作OS
OMGR/MGR	Windows Server(R) 2003 Enterprise Edition SP2
OMGR/Client	Windows(R) XP Professional SP2

（３）TOE の動作構成

（１）にて示したTOEは、図 2-1で示すように各サーバおよび管理クライアントに適用され、TOEの論理的な機能（2.3.3 を参照のこと）を提供する。なお、本TOEは外部ネットワークからのアクセスから保護された、内部ネットワーク環境での運用を想定する。

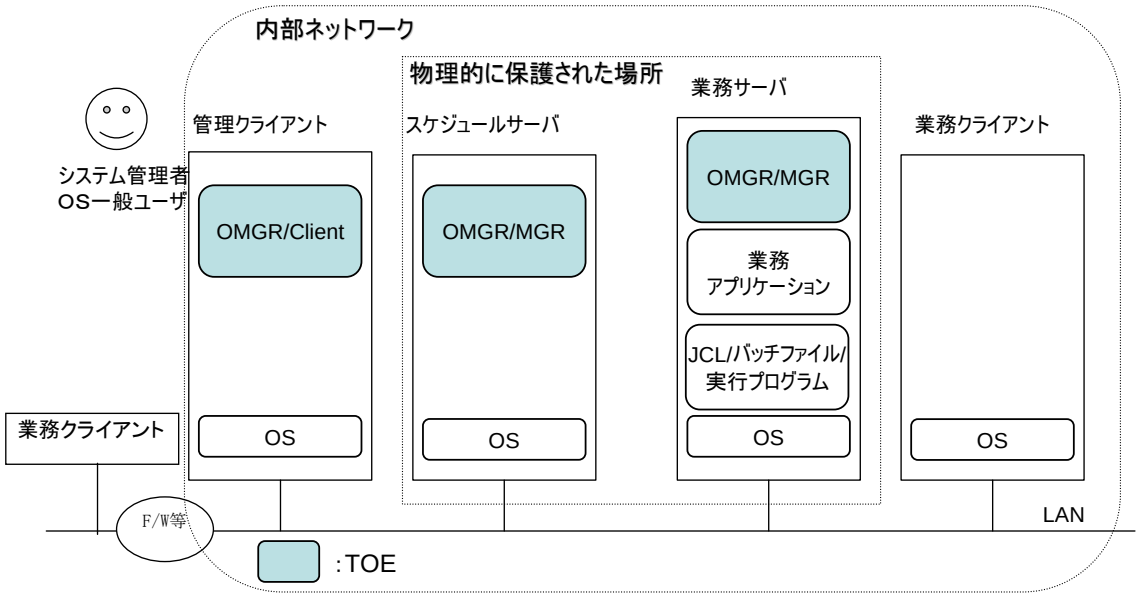

図 2-1　TOE の基本的な動作環境

OMGR/MGR は、サーバ機器の役割に関係無く同一のソフトウェアが導入され、導入後の環境設定により役割が決定されるため、「スケジュールサーバ」および「業務サーバ」に適用される TOE には、ソフトウェア構成としての違いはない。

・各構成の接続について

サーバ、クライアントの接続関係（各サーバ、クライアントには、どのクライアントまたはサーバが接続される可能性があるか）を示す。

表 2-3　サーバ、クライアントの接続関係

接続可能なサーバ／クライアント ＼ サーバ、クライアント	管理クライアント	業務クライアント	スケジュールサーバ	業務サーバ
管理クライアント		×	○	×
業務クライアント	×		×	○
スケジュールサーバ	○	×		○
業務サーバ	×	○	○	

表 2-3に示すサーバ、クライアントの接続関係がすべての接続である。これらが複数構成（例えば、１つのスケジュールサーバに、複数の業務サーバが接続される等）になった場合でも、ネットワーク間に流れるデータの種類は同じであり、また、ネットワーク接続の仕組み自体も同じである。そのため、複数構成による、新たな不正利用の脅威は発生しない。

以下に、各サーバの概要を説明する。なお、スケジュールサーバ、及び業務サーバは、システム管理者以外が入退室できない、物理的に保護された場所に設置されることを想定している。

なお、以下に示すサーバは、構成により、１台で複数の役割を兼ねる場合がある。例えば、１台でスケジュールサーバ及び業務サーバの役割を兼ねる等。

スケジュールサーバ

スケジュールサーバは、業務サーバに対する自動運転用定義情報の管理による、ジョブのスケジューリングを主に行うサーバである。本サーバへの操作は、管理クライアント及びサーバへのコマンドの直接投入により行なう。本サーバには、OMGR/MGR が適用される。

業務サーバ

業務サーバは利用者のアプリケーションを実行するサーバである。本サーバはスケジュールサーバからの指示を受けてジョブの実行を制御する。

業務サーバ上の OMGR/MGR はスケジュールサーバに適用されたものと同一であり、設定によって上記の動作を行う。

本サーバには、OMGR/MGR が適用される。

以下に示す管理クライアント及び業務クライアントは、クライアントであるため、システム管理者以外が入退室できない、物理的に保護された場所に設置する必要はない。

また、管理クライアントの利用は、内部ネットワーク内に限定されるが、業務クライアントは外部ネットワークに設置しても良い。

管理クライアント

管理クライアントは、スケジュールサーバおよび業務サーバの動作を規定する際に利用するクライアントである。システム管理者、OS 一般ユーザが使用する。本クライアントには、OMGR／Client が適用される。

なお、管理クライアントを使用して、TOE に対する操作を行なう方法は以下がある。

・GUI(クライアント機能)による操作

・CUI(コマンド)による操作

なお、GUI に関しては、TOE のクライアント機能が提供する。一方、CUI(コマンド)に関しては、IT 環境の OS が提供する。

業務クライアント

業務クライアントは、一般利用者が業務サーバにアクセスし、業務アプリケーションを利用した業務を行なう際に使用するクライアントである。但し、TOE は導入されない

2.3.2 TOEの関係者

本節では、TOE の関係者について説明する。なお、TOE の関係者を説明するに当たり、まず、TOE に関係する権限について説明する。

表 2-4 TOE に関係する権限

権限		権限説明
使用環境の権限	組織の責任者権限	業務システムに対し、運用、設置場所、人の管理において責任を有する権限である。
	機器管理権限	業務システムを構成するサーバ機器を管理する権限
TOE における権限	システム管理者権限(コマンド)	CUI(コマンド)を利用して以下を行なうことが可能となる権限である。 ・OS 一般ユーザの登録・削除 ・すべての範囲(※)で、運用管理業務を行なう ・OS 一般ユーザの、担当範囲(※)を設定する ・OS のアクセス権限を設定する ・JCL/バッチファイル/実行プログラムを作成する
	システム管理者権限(GUI)	TOE が提供する GUI(クライアント機能)を利用して、以下を行なうことが可能となる権限である。 ・すべての範囲(※)で、運用管理業務を行なう ・OS 一般ユーザの担当範囲(※)を設定する
	OS 一般ユーザ権限(コマンド)	コマンドを利用して、担当範囲(※)で、運用管理業務を行なうことが可能となる権限である。 また、JCL/バッチファイル/実行プログラムを作成可能な権限を併せて持つ。 特に、本権限を持つユーザが、自動運転用定義情報の所有者の場合、当該自動運転用定義情報に対しすべての運用管理業務を行なうことが可能となる。
	OS 一般ユーザ権限(GUI)	TOE が提供する GUI(クライアント機能)を利用して、担当範囲(※)で、運用管理業務を行なうことが可能となる権限である。 特に、本権限を持つユーザが、自動運転用定義情報の所有者の場合、当該自動運転用定義情報に対しすべての運用管理業務を行なうことが可能となる。

※「すべての範囲」とは、すべての自動運転用定義情報が対象範囲である、ということを意味する。

「担当範囲」とは、指定された自動運転用定義情報が対象範囲である、ということを意味する。

[表の説明]

使用環境の権限とは、TOE の使用環境における、物理的、人的、接続的な側面での権限である。(非 IT の権限)

TOE における権限とは、TOE の利用上の権限である。(IT の権限)

本TOEの関係者と、関係者が所有する権限について表 2-5に説明する。

表 2-5 TOE の関係者

TOE の関係者	当該関係者の説明	当該関係者が所有する権限
組織の責任者	組織の長。	[使用環境の権限] ・組織の責任者権限 [TOE における権限] ・なし
システム管理者	サーバの OS において、Administrator アカウントを有する人物。	[使用環境の権限] ・機器管理権限 [TOE における権限] ・システム管理者権限(コマンド) ・システム管理者権限(GUI)
OS 一般ユーザ	サーバの OS の Administrator 以外のアカウントを有する人物。	[使用環境の権限] ・なし [TOE における権限] ・OS 一般ユーザ権限(コマンド) ・OS 一般ユーザ権限(GUI)
一般利用者	業務クライアントを利用して業務を行なう人物。	[使用環境の権限] ・なし [TOE における権限] ・なし

2.3.3 TOEの論理的構成

TOEは表 2-6の機能単位から構成される。

表 2-6 TOE の論理的構成

区分	名称	OMGR/MGR	OMGR/Client
サーバ機能	カレンダ機能	○	
	電源制御	○	
	アプリケーション起動	○	
	ジョブスケジューラ	○	
	ジョブ実行制御	○	
	支援機能	○	
	スケジュール分散機能	○	
	稼動ログ管理機能	○	
	通信機能	○	
	ポリシー配付機能	○	
	ジョブ再実行機能	○	
	ジョブの状態確認機能	○	
	イベント監視機能	○	
	アクション管理機能	○	
	バックアップ連携機能	○	
クライアント機能	クライアント機能		○
セキュリティ機能	アクセス制御機能	○	
	監査ログ出力機能	○	
	パスワード保護機能	○	○

凡例）○：含まれていることを示す

サーバ機能およびクライアント機能は、業務システムの自動運転を直接支援する機能を提供する。TOEの物理的構成要素であるOMGR/MGR、OMGR/Clientは、表 2-6に示す通り、各サーバ機能、クライアント機能、セキュリティ機能を提供する。

2.4 サーバ機能およびクラアント機能

表 2-6に示したサーバ機能およびクライアント機能の詳細を以下に示す。

2.4.1 カレンダ機能

本機能は、平日（運用日）、休日などの運用情報を定義するための機能である。自動運転用定義情報にて定義した情報をアプリケーション起動、ジョブスケジューラで参照させることにより、様々なパターン（例えば、平日と休日で起動するアプリケーションを変えるなど）でシステムを運用することが可能になる。

2.4.2 電源制御

本機能により、サーバの電源投入、切断、リブートの契機を自動運転用定義情報にて定義し、定義した時刻になると、電源制御機能は電源制御装置と連携して、サーバの電源を自動的に投入/切断またはリブートする。但し、ジョブの自動運転のためには、本機能の利用は特に、必須というものではない。そのため、本機能の連携対象である電源制御装置についても、本 TOE が動作する構成としては必須のものではない。

2.4.3 アプリケーション起動

本機能により、サービスを起動した後に、あらかじめ起動するアプリケーションとその起動順序を指定したアプリケーションスケジュール（自動運転用定義情報にて定義される）に従って、アプリケーションを自動的に起動する。起動したアプリケーションは、電源を切断する前に、起動とは逆の順序で終了させる。日によって異なる業務環境を構築することが可能となる。

2.4.4 ジョブスケジューラ

本機能は、業務システム全体の業務について、スケジュールから監視・制御までの操作をジョブ間の制御を効率的に行うことで簡素化する。ジョブの起動および強制終了の機能は、本機能にて提供される。

なお、本機能にて、ジョブ間の制御を行ない、後述する「ジョブ実行制御」で、ジョブ単位の効率的な実行制御を行なう。

2.4.5 ジョブ実行制御

本機能は、ジョブスケジューラにより投入されたジョブに対し、実行から終了までを効率的に制御する機能を提供する。

2.4.6 支援機能

本機能は、サーバとサーバ間またはサーバとクライアント間での業務データなどのやりとりを、コマンドで実行できるようにする機能である。ファイルの操作や、転送、圧縮/伸長、またアプリケーションの起動やクライアントの電源投入/切断の制御処理を可能とする。

2.4.7 スケジュール分散機能

本機能により、スケジュールを、運用日ごとに管理・運用することができる。運用日ごとにスケジュールが管理できるため、マスタスのスケジュールを変更することなく定義を変更できる。

2.4.8 稼動ログ管理機能

本機能により、「ジョブ実行制御機能」および「ジョブスケジューラ」から通知された、業務サーバが起動した起動結果及び処理結果が、ジョブの実行記録として出力される。

2.4.9 通信機能

本機能により、サーバ間の通信、及びサーバクライアント間の通信が可能となる。なお、本機能におけるネットワーク上のデータへのインタフェースは、非公開である。

2.4.10 ポリシー配付機能

本機能は、既存のサーバにある自動運転用定義情報、アクセス制御情報、及びジョブ所有者情報の定義から情報を抽出して、新規に導入するサーバに配付、適用する機能を提供する（この情報を「ポリシー情報」と呼ぶ。）本機能によりポリシー情報を抽出、配付、適用することで、すでに運用中のサーバと同じ運用環境を新規のサーバ上にも構築することができる。

ポリシー情報に含まれる情報としては、以下の情報がある

- 管理対象となるホスト名
- ジョブ所有者情報の定義
- アクセス制御機能に関する情報
- アクション管理機能に関する情報
- イベント監視機能に関する情報
- カレンダ機能に関する情報
- アプリケーション起動に関する情報
- ジョブスケジューラで登録したスケジュール

なお、上記には、機密情報は含まれていない。

2.4.11 ジョブ再実行機能

本機能は、以下の機能を提供する。

・リカバリジョブを自動運転用定義情報に登録する機能

・事前にリカバリジョブを登録しておくことで、実行中のジョブが異常終了した際に再実行する機能(自動再実行)

・手動でジョブを再実行する機能(手動再実行)

※自動再実行をサポート（自動再実行では復旧できない障害の対処）する目的で、手動の再実行機能を提供している。なお、手動再実行だけであると、運用管理が煩わしくなるため、自動再実行を提供している。

2.4.12 ジョブの状態確認機能

本機能は、ジョブが現在どの様な状態(正常状態・異常状態)なのかをタイムリに確認する機能を提供する。

2.4.13 イベント監視機能

本機能は、「システム異常を知らせるメッセージの出力」などのイベントが発生した時に、ポケットベルの呼び出しやメール送信といったアクションを、人手を介さずに自動的に行う機能を提供する。自動的に実行するアクションは、平日や休日、あるいは時間帯によって替えることができる。

2.4.14 アクション管理機能

本機能は、イベント監視機能によって自動実行される音声通知、メール送信、ポップアップメッセージ通知およびポケットベル通知の処理の、一時停止/優先順位の変更/アクションの停止などの処理を行なう機能を提供する。

2.4.15 バックアップ連携機能

本機能は、データを自動バックアップするプログラムである ARCserve の機能を、コマンドを使って利用できるようにする。本機能の実行のためには、ARCserve が必須である。

2.4.16 クライアント機能

前述のサーバ機能に対する GUI による操作インタフェースを、システム管理者及び OS 一般ユーザに提供する。

2.5 TOEのセキュリティ機能

本 TOE が提供するセキュリティ機能は以下である。

・アクセス制御機能

・監査ログ出力機能

・パスワード保護機能

2.5.1 アクセス制御機能

本機能は、以下の機能を提供する。

・OS 一般ユーザの自動運転用定義情報に対する操作を、許可された範囲に制限する機能

本機能は、「アクセス制御情報」という定義情報を基にした制御により実現される。

なお、ジョブは OS 上で動作するため、(自動運転用定義情報からの) ジョブの実行は、OS ユーザの権限で行なわれる。この際、ジョブの実行ユーザが「ジョブ所有者情報の定義」に登録されている OS ユーザ以外であった場合、そのジョブの実行は拒否される。

OS 一般ユーザに対する「アクセス制御機能」の動作イメージを図示する。

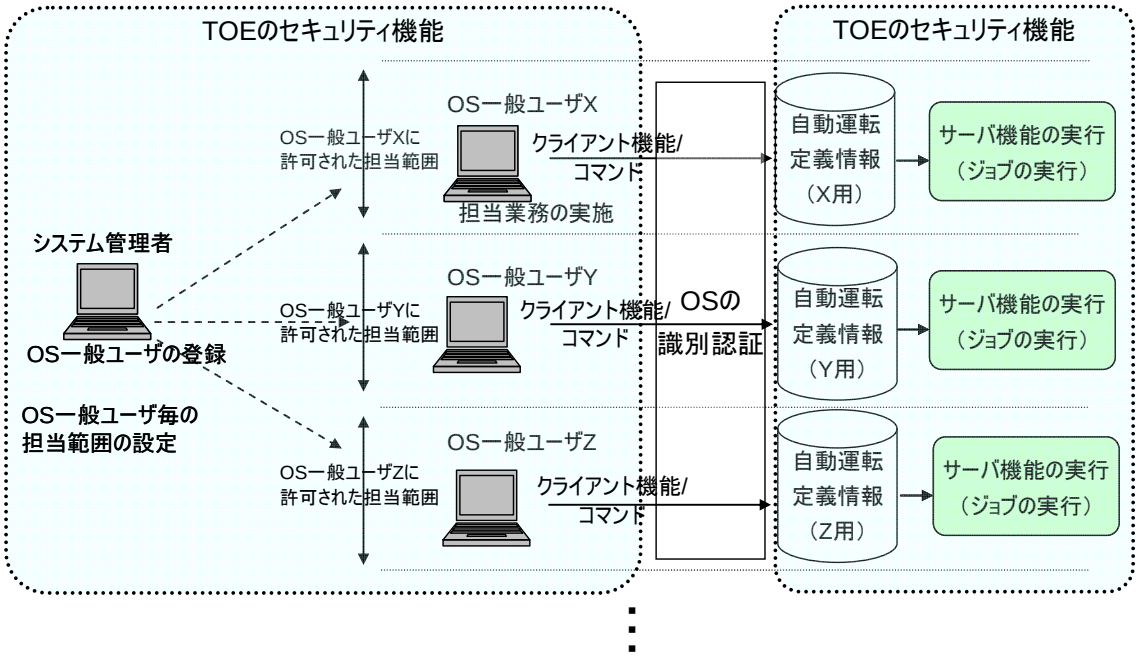

図 2-2　セキュリティ機能の動作イメージ

[図の説明]

「アクセス制御機能」は、OS 一般ユーザの操作を、許可された担当範囲に制限する機能がである。(詳細は、2.5.1 を参照)

システム管理者はコマンドを使用して、OS 一般ユーザの登録を行う。
システム管理者は、OS ユーザ(ジョブの実行ユーザ)を「ジョブ所有者情報の定義」に指定する。
システム管理者は、コマンドまたは GUI(クライアント機能)を使用して、OS 一般ユーザの担当範囲（「アクセス制御情報」に基づく）の設定を行なう。OS 一般ユーザは OS の識別認証機能による識別認証の後、コマンドまたは GUI(クライアント機能)を使用して、OS 一般ユーザに許可された範囲内で自動運転用定義情報にジョブのスケジュールを行う。ジョブは、その定義されたスケジュールに基づき OS ユーザの権限で動作を行なう。

なお、システム管理者は、自動運転用定義情報に対し、業務上の責任者として「所有者」を設定する。所有者として設定された OS 一般ユーザは、当該自動運転用定義情報に対しすべての運用管理業務を行なうことが可能となる。

2.5.2 監査ログ出力機能

本機能はアクセス制御機能に関する記録を監査ログとして採取し、監査ログファイルに出力する機能を提供する。

2.5.3 パスワード保護機能

本機能は、内部ネットワーク上に流れるパスワードを保護する機能を提供する。

2.6 TOEの機能間の関係

本節では、2.4、2.5 にて示した TOE の機能間の関係について説明する。

図 2-3に、管理クライアント、スケジュールサーバ、業務サーバでの構成で構築した環境における、TOEの機能間の関係を図示する。なお、下図において網掛けした機能は、当該サーバ上において利用されない機能である。

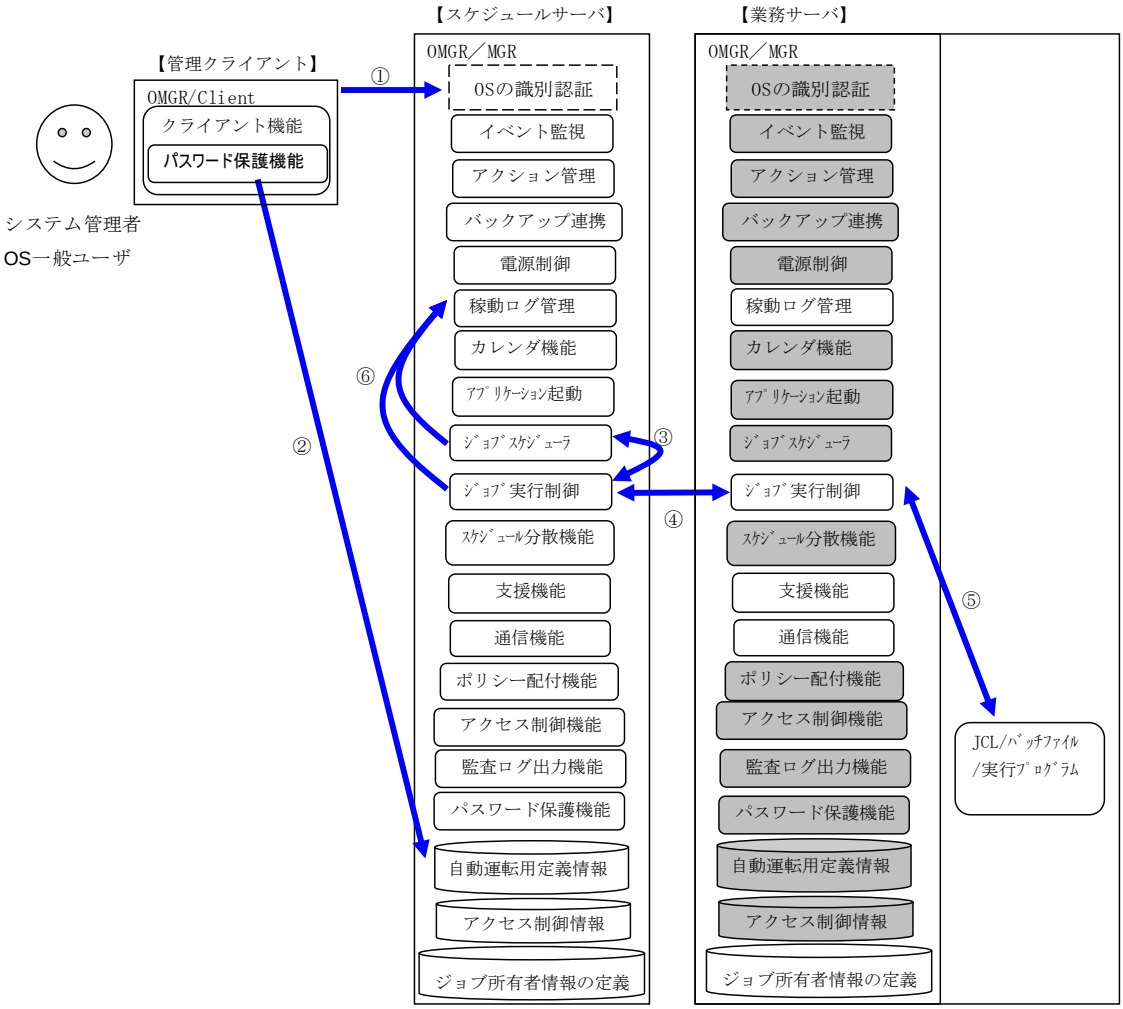

図 2-3　本 TOE の機能間の関係

[図の説明]

システム管理者、OS 一般ユーザは、OMGR/Client の操作メニューから、スケジュールサーバの OMGR／MGR に対してアクセスする。その際、OS の識別認証が行なわれる（図中①）

OS の識別機能により、システム管理者または OS 一般ユーザである事が確認された場合は、OMGR/Client の操作メニューを利用して、運用管理に必要な各種の環境操作を行う。

環境操作では、システム管理者は、OS 一般ユーザの操作範囲を許可された範囲に制限する設定、イベント監視設定、アクション管理設定、バックアップ連携設定、カレンダ設定、

ジョブの実行スケジュール定義を行う。設定した情報は、自動運転用定義情報に格納される。(図中②)

自動運転（ジョブ起動）は、スケジュールサーバのジョブスケジューラが、自動運転用定義情報に設定されたスケジュールに従い、同じスケジュールサーバのジョブ実行制御に対して起動依頼を出す。その後、ジョブ実行制御が業務サーバのジョブ実行制御に対して起動依頼を伝達する。それに伴い、業務サーバのジョブ実行制御が、対象のジョブ（JCL/バッチファイル/実行プログラム）を起動する事により、ジョブの計画的な実行を実現している。なお、ジョブの実行はジョブの実行ユーザの権限で行なわれるが、この際、ジョブの実行ユーザが「ジョブ所有者情報の定義」に登録されている OS ユーザ以外であった場合、そのジョブの実行は拒否する。(図中③～⑤)

ジョブの起動結果および処理結果は、逆の経路でスケジュールサーバのジョブ実行制御およびジョブスケジューラに通知される。また業務サーバが稼動した起動結果および処理結果はジョブの実行記録として管理される。(図中⑥)

この運用環境に対して、本 TOE は、システム管理者および OS 一般ユーザが自動運転用定義情報の操作を行う部分（図中②）に、不正な操作を防止するアクセス制御機能を用意することで、セキュアな運用管理を実現する。このアクセス制御機能は、アクセス制御情報に基づき制御が行なわれる。

コマンドを使用した OS 一般ユーザによる業務実行も、クライアント機能を使用しないこと以外、違いはない。

なお、上記の利用準備として、システム管理者は OS ユーザの登録を行なう。

2.7 IT環境

本 TOE は、IT 環境に対し、サーバへのコマンド投入するための CUI を要求する。

本 TOE は、IT 環境に対し、コマンドおよび GUI を使用するシステム管理者、コマンドおよび GUI を使用する OS 一般ユーザが正当な人物であるかを識別認証する機能を必要とする。

また、監査ログを閲覧する機能、及び監査ログファイルを保護する機能を必要とする。

TOE としては、監査ログ出力機能の起動と終了の事象を監査ログに採取しないため、OS に対し、当該事象を採取する機能を必要とする。また、OS は監査ログのために、時刻を提供する。

2.8 環境に対する運用

システム管理者は、TOE を動作させる事前設定として、悪意のあるものがサーバ上の OS から直接 TOE で扱う資源(2.9 を参照)にアクセスできないように、OS のアクセス権設定を行なう必要がある。

また、コマンドを使用する際には、内部ネットワークに流れるパスワードに対する盗聴、暴露から保護できるようなアクセス手段を採用する必要がある。

2.9 保護資産

TOE が保護すべき資産（処理）は、ジョブの計画的な実行である。本 TOE においてジョブの計画的な実行は「自動運転用定義情報」にて定義され、その定義に従い「JCL/バッチファイル/実行プログラム」を実行し、「実行ジョブ」により動作される。但し、TOE として保護できるものは自動運転用定義情報」のみであり、「JCL/バッチファイル/実行プログラム」及び「実行ジョブ」に関しては、プラットフォームである OS で保護される資源となる。そのため、本 TOE での保護資産は、「自動運転用定義情報」である。

表 2-7において、本TOEで扱う資源について説明する。

表に示すとおり、TOE の保護資産は、「自動運転用定義情報」および「パスワード」である。まず、これら保護資産に対する保護の観点について説明する。

・パスワード

パスワードに関しては、機密情報が含まれるため、機密性を保証する必要がある。また、強度の弱いパスワードに変更される行為は、TOE のセキュリティ強度(識別認証)を弱体化させることに繋がるため、本資産には、完全性の保証が併せて必要となる。

なお、本資産は、常に使用可能としなければならないものではないため、可用性を保証する必要はない。そのため、本資産に対し、「機密性」「完全性」「可用性」の内、「機密性」「完全性」の観点での保証が必要である。

・自動運転用定義情報

自動運転用定義情報に関しては、機密情報が含まれず、また、常に使用可能としなければならないものではないため、可用性を保証する必要はない。そのため、これら資源に対し、「機密性」「完全性」「可用性」の内、「完全性」の観点での保証が必要である。

なお、これら保護資産は TOE の制御内と内部ネットワーク上に存在する。攻撃者が意図した通りに保護資産を改ざんするためには、TOE の内部仕様を理解した上で非公開のインタフェースを使用して攻撃する必要がある。そのため、低レベルの攻撃者では不可能であり、TOE としては、ネットワーク上での保護資産に対し完全性保証のための機構を導入しない。

次に、保護資産以外の、TOE で利用する資源の扱いについて説明する。

- JCL/バッチファイル/実行プログラム
- 実行ジョブ
- ジョブの実行記録
- 監査ログファイル

これらの資源には、機密性以外の、「可用性」(対象は実行ジョブ)、「完全性」(対象は、

JCL/バッチファイル/実行プログラム、ジョブの実行記録、および監査ログファイル）の観点での保証が必要であるが、それらは、TOE の制御内で対処できるものではなく、プラットフォームである OS でのアクセス権設定により保護が可能となる。

表 2-7にて網掛けしている「自動運転用定義情報」および「パスワード」がTOEの保護資産である。

表 2-7　TOE で扱う資源

資源		説明
ジョブの計画的な実行	自動運転用定義情報	ジョブの計画的な実行を行なう際に利用する定義情報である。 この定義情報には、業務システムが行うサービスの開始や終了に影響を与えるシステムの運転情報が含まれており、計画どおり安定的に業務システムを稼動させるためには、完全性を保証する必要がある。 TOE は OS 一般ユーザに対し、本資産を変更（運用管理）するインタフェースを提供しているため、不正な改変行為から保護する機構を導入する必要がある。
	JCL/バッチファイル/実行プログラム	ジョブを起動、終了する際に利用される情報である。ジョブの計画的な実行を実現するためには、TOE を経由した本資源の不正な利用を制限する必要がある。 但し、本資源に対しては OS 経由でのアクセスが可能であるため、不正な利用を防止するために、OS のアクセス権設定により許可された役割のみに制限を行なう必要がある。
	実行ジョブ	スケジュールに基づき実行される、または、実行中のジョブ自体である。 ジョブの計画的な実行のためには、ジョブ自体に対し、スケジュールに従った正しい動作が要求される。
ジョブの実行記録		ジョブの実行記録である。本記録の中には業務アプリケーションが出力したメッセージが存在しているため、完全性を保証する必要がある。（業務アプリケーションが出力するメッセージには、機密情報は含まれていない。） 本資源については、TOE としては「ジョブ実行制御機能」/「ジョブスケジューラ」から「稼動ログ管理機能」を介し生成するインタフェースのみ提供し、直接編集するインタフェースを提供していない。そのため、TOE として本資源を保護するための機構は不要である。但し、本資源に対しては OS 経由でのアクセスが可能であるため、完全性を保証するために、OS のアクセス権設定により許可された役割（システム

	管理者）のみに制限を行なう必要がある。
監査ログファイル	監査ログ出力機能にて出力されるファイル。本ファイル内には、アクセス制御機能に関する記録が採取されている。但し、これらには、機密情報はなく、完全性の保証のみが必要となる。 本資源には、TOE としては「アクセス制御機能」を契機として監査の記録を採取するインタフェースのみ提供し、直接編集するインタフェースを提供していない。そのため、TOE として本資源の完全性を保護するための機構は不要である。但し、本資源に対しては OS 経由でのアクセスが可能であるため、完全性を保証するために、OS のアクセス権設定により許可された役割（システム管理者）のみに制限を行なう必要がある。
パスワード	システム管理者および OS 一般ユーザを認証するためのデータである。本データに対しては機密性、完全性の保証が必要である。

ジョブの計画的な実行を、時系列を基に説明する。

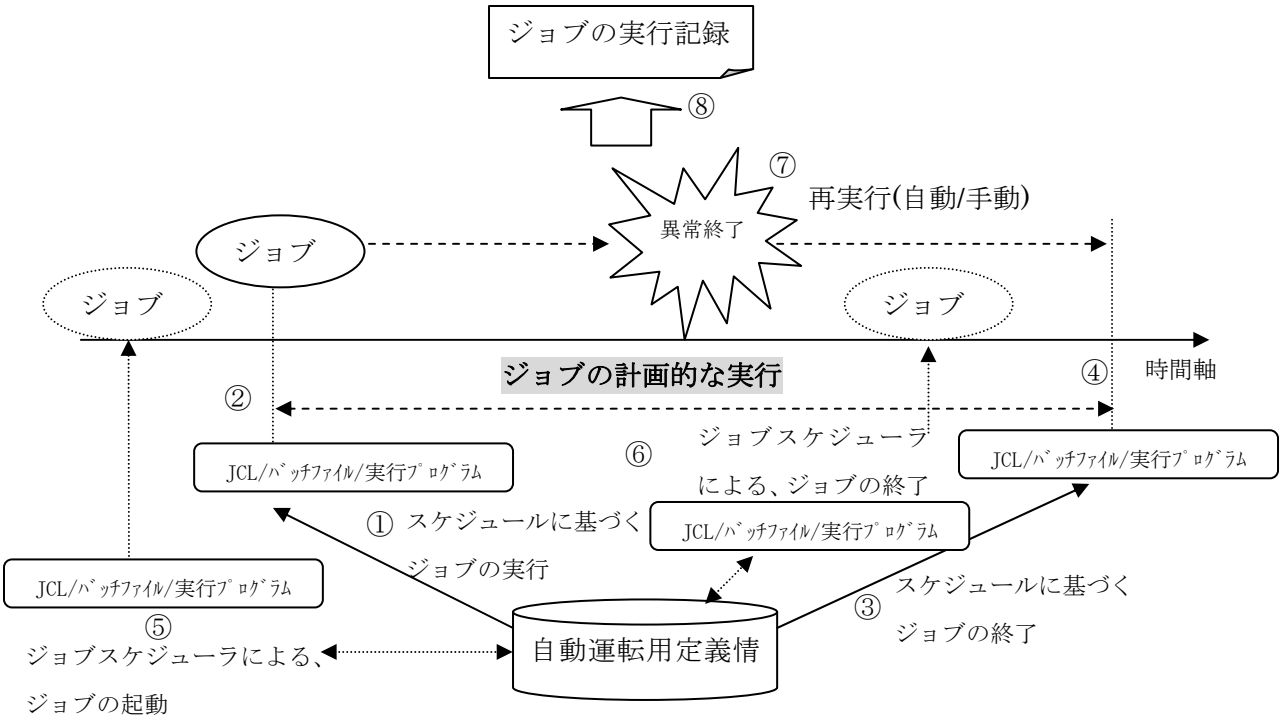

図 2-4　ジョブの計画的な実行

[図の説明]

ジョブの計画的な実行は、自動運転用定義情報のスケジュールを基に JCL/バッチファイル/実行プログラムを起動、終了することで実現する。

①は、自動運転用定義情報のスケジュールに基づき JCL/バッチファイル/実行プログラムの実行命令（起動）が行われることを示している。

②は、JCL/バッチファイル/実行プログラムに基づきジョブが起動されることを示している。

③は、自動運転用定義情報のスケジュールに基づき JCL/バッチファイル/実行プログラムの実行命令（終了）が行われることを示している。

④は、JCL/バッチファイル/実行プログラムに基づきジョブが終了されることを示している。

⑤は、ジョブスケジューラにより、JCL/バッチファイル/実行プログラムの実行命令(起動)が行なわれることを示している。

⑥は、ジョブスケジューラにより、JCL/バッチファイル/実行プログラムの実行命令(強制終了)が行なわれる行なわれることを示している。

なお、ジョブスケジューラの操作対象が、スケジュールジョブであるため、操作は自動運

転用定義情報を参照した後に実行される。

また、実行中にジョブが異常終了した場合は、TOE は当該ジョブを再実行する。

⑦は、ジョブが異常終了した事象を示している。

⑧は、ジョブが実行した記録が、ジョブの実行記録として出力されることを示している。

3 TOEセキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1 前提条件

本 TOE には意図する使用方法及び使用環境に関して、以下の前提条件が存在する。

■ A.ADMIN（システム管理者の信頼性）

システム管理者は、不正な操作を行わない信頼できる人物であることを想定する。

■ A.PASSWORD（パスワードの管理）

パスワードの管理について、以下を想定する。

・TOE を利用する OS 一般ユーザのパスワードは、システム管理者及び本人以外に知られないように管理される。

■ A.PLACE（設置場所）

本 TOE が動作するサーバは、システム管理者以外が入退出できない、事務フロアやサーバルーム等に設置されることを想定する。

■ A.NETWORK（ネットワーク環境）

本 TOE は、外部ネットワークから直接アクセスされないイントラネット環境にて動作されることを想定する。

■ A.OS_ACCESS(OS を経由したアクセス)

悪意のある者により、本 TOE を介さず、直接サーバ上の OS から TOE で扱う資源にアクセスできないよう、OS のアクセス権設定されることを想定する。

3.2 脅威

本 TOE には意図する使用方法及び使用環境に関して、以下の脅威が存在する。

本 TOE では、低レベルの攻撃者を想定する。

■ T.PASSWORD_TAP（パスワードの盗聴）

悪意のある者は、内部ネットワーク上に流れるパスワードを盗聴し、内容を暴露するかもしれない。

■ T.UAUSER_CLIENT（クライアント機能を使用時のなりすまし）

悪意のある者は、クライアント機能を使用して、システム管理者、及び OS 一般ユーザになりすまし、自動運転用定義情報の改ざんを行い、ジョブの計画的な実行を阻害するかもしれない。

■ T.UAUSER_COMMAND（コマンドを使用時のなりすまし）

悪意のあるものは、コマンドを使用して、システム管理者、OS 一般ユーザになりすまし、自動運転用定義情報の改ざんを行い、ジョブの計画的な実行を阻害するかもしれない。

■ T.UAACTION（許可されない操作）

OS 一般ユーザとして識別認証されたものは、クライアント機能またはコマンドを使用してシステム管理者が許可した担当範囲を超えて操作を行い、自動運転用定義情報の改ざんを行い、ジョブの計画的な実行を阻害するかもしれない。

3.3 組織のセキュリティ方針

本 TOE には、組織のセキュリティ方針はない。

4 セキュリティ対策方針

本章では、TOE セキュリティ対策方針、環境のセキュリティ対策方針について記述する。

4.1 TOEのセキュリティ対策方針

本節は、脅威に対抗するための TOE のセキュリティ対策方針を示す。

■ O.PW_PROTECT（パスワードの保護）

本 TOE は、クライアント機能を使用時に、内部ネットワーク上に流れるパスワードを解析できないようにしなければならない。

■ O.PERMIT_USE（許可された範囲内での制限）

本 TOE は、OS 一般ユーザに対し、システム管理者が許可した範囲でのみ自動運転用定義情報への操作を可能とする。許可された範囲以外の操作を行おうとした場合は、その操作を拒否する。

4.2 環境のセキュリティ対策方針

脅威に対抗するための技術的な環境のセキュリティ対策方針を以下に示す。

■ OE.OS_I&A（OS の識別認証）

OS は、クライアント機能を使用したシステム管理者及び OS 一般ユーザを識別認証する。また、OS はコマンドを使用したシステム管理者及び OS 一般ユーザを識別認証する。識別と認証が失敗した場合には、本 TOE の利用を拒否する。

■ OE.AUDIT（監査の実施）

IT 環境は、本 TOE に対する不正な兆候がないかを確認するための監査ログを閲覧する機能、及び監査ログファイルを保護する機能を提供する

■ OE.OS_AUDIT（監査の起動と終了事象の採取）

OS は、TOE の監査ログ出力機能の起動と終了の事象を採取する機能を提供する。
また、OS は監査ログに使用する時刻を提供する。

■ OE.ATTRIBUTE(利用者と利用者プロセスの結合)

OS は、TOE が行う OS 一般ユーザに対する許可された範囲での自動運転用定義情報への操作制限をサポートする目的で、OS 一般ユーザと利用者プロセスとの結合を行う。

前提条件を実現するための非技術的な環境のセキュリティ対策方針を以下に示す。

■ OE.ASSIGN（選任）

組織の責任者は、システム管理者として信頼できる人物を選任すると共に、不正を行なわないように教育を行なわなければならない。

■ OE.PASSWORD（パスワードの管理）

システム管理者は、TOE を利用する OS 一般ユーザに対し、自身のパスワードを他に漏洩しないように管理する事を教育し、遵守させなければならない。

■ OE.PLACE（設置場所）

システム管理者は、本 TOE が動作するサーバを、人的、機械的又は電子的な手段による入退出管理が施された、システム管理者以外が容易に入室不可能な事務フロアやサーバルーム等に設置しなければならない。

■ OE.NETWORK(内部ネットワーク環境)

システム管理者は、本 TOE が動作するサーバ、クライアントをネットワークに接続する場合、ファイアウォール等で区切られたイントラネット内に接続しなければならない。

■ OE.OS_SETUP(OS のアクセス設定)

システム管理者は、本 TOE を介さず、直接 OS から TOE で扱う資源に不正を行なわないよう、サーバ上の OS のアクセス権設定を行なわなければならない。

■ OE.COMMAND_ACCESS(コマンド使用時の運用)

システム管理者及び OS 一般ユーザが、コマンドを使用時に、悪意のあるものに内部ネットワーク上に流れるパスワードが解析されないように、SSH を利用しなければならない。

5 ITセキュリティ要件

本章では、TOE セキュリティ要件、IT 環境に対するセキュリティ要件、セキュリティ機能強度を示す。

5.1 TOEセキュリティ要件

5.1.1 TOEセキュリティ機能要件

FAU_GEN.1 監査データ生成

下位階層: なし

FAU_GEN.1.1

TSFは、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査の[選択: *最小、基本、詳細、指定なし: から一つのみ選択*] レベルのすべての監査対象事象; 及び

b) [割付: *上記以外の個別に定義した監査対象事象*]

[選択: *最小、基本、詳細、指定なし: から一つのみ選択*]

・最小

表5-1に監査の対象を示す。

表 5-1 監査の対象

機能要件	CC で定義された監査対象	監査事象
FAU_GEN.1	予見される監査対象事象はない。	―
FAU_STG.3	a)基本:閾値を超えたためにとられるアクション	最小を選択しているため、適用外。
FDP_ACC.1	予見される監査対象事象はない。	―
FDP_ACF.1	a) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細: アクセスチェック時に用いられ	・自動運転用定義情報に対する操作の成功事象 但し、参照の成功事象に関しては、監査ログを採取しない(自動運転用定義情報には、機密情報は含まれないた

機能要件	CC で定義された監査対象	監査事象
	る特定のセキュリティ属性。	め)
FMT_MOF.1	a) 基本: TSFの機能のふるまいにおけるすべての改変。	最小を選択しているため、適用外。
FMT_MSA.1	a)基本: セキュリティ属性の値の改変すべて。	最小を選択しているため、適用外。
FMT_MSA.3	a)基本:許可的あるいは制限的規則のデフォルト設定の改変 b)基本:セキュリティ属性の初期値の改変すべて。	最小を選択しているため、適用外。
FMT_MTD.1	a) 基本: TSFデータの値のすべての改変	最小を選択しているため、適用外。
FMT_SMF.1	a) 最小：管理機能の使用	以下の管理機能の使用（注） ・OS 一般ユーザに関係するオブジェクト属性(OS 一般ユーザのアクセス権)の登録・改変・削除機能 ・所有者名の登録・改変機能 (注) 「監査ログ出力機能を起動・停止する機能を使用した際のログ」に関しては、「監査機能の起動・停止のログ」を採取しているため、それが代替となる。
FMT_SMR.1	a) 最小: 役割の一部をなす利用者のグループに対する改変; b) 詳細: 役割の権限の使用すべて。	なし （役割の一部をなす利用者のグループに対する改変が行なえないため。）
FPT_ITT.1	予見される監査対象事象はない。	―
FPT_RVM.1	予見される監査対象事象はない。	―
FPT_SEP.1	予見される監査対象事象はない。	―

[割付: *上記以外の個別に定義した監査対象事象*]

なし

FAU_GEN.1.2

TSFは、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗); 及び

b) 各監査事象種別に対して、PP/STの機能コンポーネントの監査対象事象の定義に基づいた、[割付: *その他の監査関連情報*]

[割付: *その他の監査関連情報*]

なし

依存性: FPT_STM.1 高信頼タイムスタンプ

FAU_STG.3 監査データ損失の恐れ発生時のアクション

下位階層： なし

FAU_STG.3.1

TSF は、監査証跡が[割付：*事前に定義された限界*]を超えた場合、[割付：*監査格納失敗の恐れ発生時のアクション*]をとらなければならない。

[割付：*事前に定義された限界*]
・監査ログファイルの有効期限

[割付：*監査格納失敗の恐れ発生時のアクション*]
・古い日付の監査ログファイルの削除

依存性： FAU_STG.1 保護された監査証跡格納

FDP_ACC.1 サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1

TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。

[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]

表 5-2に示す

表 5-2　サブジェクト、オブジェクト、操作のリスト

サブジェクト	オブジェクト	操作
利用者プロセス	・自動運転用定義情報	参照 操作 更新 登録

[割付: *アクセス制御 SFP*]

- 自動運転用定義情報アクセス制御 SFP

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1

TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。

[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]
表 5-3および表 5-4に示す

表 5-3　サブジェクト、オブジェクト

サブジェクト	オブジェクト
利用者プロセス	・自動運転用定義情報

表 5-4　自動運転用定義情報アクセス制御 SFP に関わるセキュリティ属性のリスト

サブジェクト属性	オブジェクト属性
・OS ユーザ名 ・権限属性	●自動運転用定義情報のオブジェクト属性 アクセス制御情報内に記載される以下の情報が、オブジェクト属性となる。なお、アクセス制御情報は、所有者毎に作成される。 ・所有者名 ・OS 一般ユーザに対するアクセス権（OS ユーザ名・アクセス権レベル）

[割付: *アクセス制御 SFP*]

- 自動運転用定義情報アクセス制御 SFP

FDP_ACF.1.2

TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: 制御され

たサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

[割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]
表 5-5に示す

表 5-5　自動運転用定義情報アクセス制御 SFP の規則

自動運転用定義情報アクセス制御 SFP の規則
【分岐条件】 ・権限属性が「OS一般ユーザ」である、かつ ・「所有者名」と「OSユーザ名」が一致しない 【アクセス制御規則】 サブジェクト属性である「OSユーザ名」と、「OS一般ユーザに対するアクセス権」における「OSユーザ名」が一致している場合、当該自動運転用定義情報に対し「OS一般ユーザに対するアクセス権」のアクセス権レベルに従った操作が許可される。

FDP_ACF.1.3

TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。

[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]
・権限属性が「OS一般ユーザ」である、かつ、「所有者名」とサブジェクト属性の「OSユーザ名」が一致している場合、当該自動運転用定義情報へのすべての操作が許可される。
・権限属性が、「システム管理者」である場合、すべての自動運転用定義情報に対し、すべての操作が許可される。

FDP_ACF.1.4

TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアク*

セスを明示的に拒否する規則]

なし

依存性: FDP_ACC.1 サブセットアクセス制御

FMT_MSA.3 静的属性初期化

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

FMT_MOF.1.1

TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。

[割付: *機能のリスト*]

表 5-6に示す

[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]

表 5-6に示す

[割付: *許可された識別された役割*]

- システム管理者役割

表 5-6　機能のリストとふるまいの対応

セキュリティ機能	[選択: のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]
監査ログ出力機能	・を停止する ・を動作させる

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_MSA.1 セキュリティ属性の管理

下位階層： なし

FMT_MSA.1.1

TSF は、セキュリティ属性[割付：*セキュリティ属性のリスト*]に対し[選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、[割付：*その他の操作*]]をする能力を[割付：*許可された識別された役割*]に制限するために[割付：*アクセス制御 SFP*、*情報フロー制御 SFP*]を実施しなければならない。

[割付：*セキュリティ属性のリスト*]

表 5-7に示す

表 5-7　セキュリティ属性のリスト

サブジェクト属性	オブジェクト属性
・OS ユーザ名 ・権限属性	●自動運転用定義情報のオブジェクト属性 アクセス制御情報内に記載される以下の情報が、オブジェクト属性となる。なお、アクセス制御情報は、所有者毎に作成される。 ・所有者名 ・OS 一般ユーザに対するアクセス権（OS ユーザ名・アクセス権レベル）

[選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、[割付：*その他の操作*]]

改変、削除

[割付：*その他の操作*]

登録

[割付：*許可された識別された役割*]

・システム管理者役割

[割付：*アクセス制御 SFP*、*情報フロー制御 SFP*]

・　自動運転用定義情報アクセス制御 SFP

役割と操作の対応を、表 5-8に示す。

表 5-8　役割と操作の対応

操作＼役割	システム管理者
OS一般ユーザに関係するオブジェクト属性(OS一般ユーザのアクセス権)の登録・改変・削除	○
所有者名の登録・改変	○

※サブジェクト属性である、OSユーザ名、権限属性に対する操作は、IT環境であるOSによって提供される。

依存性: [FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MSA.3 静的属性初期化

下位階層: なし

FMT_MSA.3.1

TSF は、その SFP を実施するために使われるセキュリティ属性として、[選択: *制限的、許可的* : *から一つのみ選択*、[割付 : *その他の特性*]]デフォルト値を与える[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。

[選択: *制限的、許可的* : *から一つのみ選択*、[割付 : *その他の特性*]]

- 許可的

[割付: *アクセス制御 SFP、情報フロー制御 SFP*]

- 自動運転用定義情報アクセス制御 SFP

FMT_MSA.3.2

TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

[割付: *許可された識別された役割*]

・システム管理者役割

依存性: FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

FMT_MTD.1 TSFデータの管理

下位階層: なし

FMT_MTD.1.1

TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去*、[割付: *その他の操作*]]する能力を[割付:*許可された識別された役割*]に制限しなければならない。

[割付: *TSF データのリスト*]
・監査ログファイルの有効期限

[選択: *デフォルト値変更、問い合わせ、改変、削除、消去*、[割付: *その他の操作*]]
改変

[割付:*許可された識別された役割*]
・ システム管理者役割

役割とTSFデータに対する操作能力の対応を表 5-9に示す。

表 5-9 役割と TSF データに対する操作能力の対応

役割	TSF データ	許可された能力
システム管理者	監査ログファイルの有効期限	・改変

依存性: FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定

下位階層： なし

FMT_SMF.1.1

TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付：*TSF によって提供されるセキュリティ管理機能のリスト*]。

[割付：*TSF によって提供されるセキュリティ管理機能のリスト*]

表 5-10に示す

表 5-10　セキュリティ管理機能のリスト

機能要件	CC で定義された管理対象	管理機能
FAU_GEN.1	予見される管理アクティビティはない。	CC で定義された管理対象事象はないが、以下の機能がセキュリティ管理機能と考えられる。 【セキュリティ管理機能】 ・監査ログ出力機能を起動・停止する機能
FAU_STG.3	a)閾値の維持 b)監査格納失敗が切迫したときにとられるアクションの維持(削除、改変、追加)	【セキュリティ管理機能】 a)有効期限の管理機能 b)なし(アクションは固定であり、管理対象とならない。)
FDP_ACC.1	予見される管理アクティビティはない。	
FDP_ACF.1	a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	CC で定義された管理対象は、「明示的なアクセス許可・拒否に基づく属性の管理」であるが、以下の機能もセキュリティ管理機能と考えられる。(以下は、明示的なアクセス許可・拒否の属性管理機能を含んでいる。) 【セキュリティ管理機能】 ・OS 一般ユーザに関係するオブジェクト属性(OS 一般ユーザに対するアクセス権)の登録・改変・削除機能 ・所有者名の登録・改変機能
FMT_MOF.1	a)TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること。	なし(役割のグループは固定)
FMT_MSA.1	a) セキュリティ属性と相互に影響を及ぼし	・なし（役割のグループは固定）

機能要件	CC で定義された管理対象	管理機能
	得る役割のグループを管理すること。	
FMT_MSA.3	a)初期値を特定できる役割のグループを管理すること b)所定のアクセス制御 SFP に対するデフォルトの許可的あるいは制限的設定を管理すること	・なし（役割のグループは固定）
FMT_MTD.1	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	・なし（役割のグループは固定）
FMT_SMF.1	予見される管理アクティビティはない。	
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	なし（役割の一部をなす利用者のグループ、役割が満たさなければならない条件は固定）
FPT_ITT.1	a)TSF が保護すべき改変の種別の管理 b)TSF の異なるパーツ間の転送中にデータ保護を提供するために使われるメカニズムの管理	a)TSF が保護するものは、「改変」ではなく「暴露」であるため、適用の対象外。 b)TSF の異なるパーツ間の転送中にデータ保護を提供するために使われるメカニズムは固定であるため、管理の必要はない。
FPT_RVM.1	予見される管理アクティビティはない。	
FPT_SEP.1	予見される管理アクティビティはない。	

依存性： なし

FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1

TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。

[割付: *許可された識別された役割*]

- システム管理者役割

FMT_SMR.1.2

TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

FPT_ITT.1 基本TSF内データ転送保護

下位階層: なし

FPT_ITT.1.1

TSFは、TSFデータがTOEの別々のパーツ間で送られる場合、TSFデータを[選択: *暴露、改変*]から保護しなければならない。

[選択: *暴露、改変*]

暴露

依存性: なし

FPT_RVM.1 TSPの非バイパス性

下位階層: なし

FPT_RVM.1.1

TSFは、TSC内の各機能の動作進行が許可される前に、TSP実施機能が呼び出され成功することを保証しなければならない。

依存性: なし

FPT_SEP.1 TSFドメイン分離

下位階層: なし

FPT_SEP.1.1

TSFは、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2

TSFは、TSC内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性: なし

5.1.2TOEセキュリティ保証要件

本ST にて要求する、TOEに対する保証レベルはEAL1 である。保証コンポーネント構成を表5-11に示す。

要求する各保証コンポーネントの保証エレメントは、CC Part3 の要求通りである。

なお、ASE クラスは、保証レベルに関わらず必須となる保証要件として採用する。

表 5-11 TOE の保証要件コンポーネント一覧

TOE セキュリティ保証要件		コンポーネント
構成管理	CM 能力	ACM_CAP.1
配付と運用	設置、生成、及び立上げ	ADO_IGS.1
開発	機能仕様	ADV_FSP.1
	表現対応	ADV_RCR.1
ガイダンス文書	管理者ガイダンス	AGD_ADM.1
	利用者ガイダンス	AGD_USR.1
テスト	独立テスト	ATE_IND.1

5.1.3 セキュリティ機能強度

TOE セキュリティ機能要件に対する最小機能強度は、SOF-基本である。また、明示された機能強度は、本 TOE の保証レベルが EAL1 ということから、AVA_SOF.1 が含まれないため主張しない。

FAU_GEN.1[E] 監査データ生成

下位階層: なし

FAU_GEN.1.1[E]

OSは、以下のTOEの監査対象事象の監査記録を生成できなければならない:
※下線部は詳細化。

a) 監査機能の起動と終了;

b) 監査の[選択: *最小、基本、詳細、指定なし: から一つのみ選択*]レベルのすべての監査対象事象; 及び

c) [割付: *上記以外の個別に定義した監査対象事象*]。

[選択: *最小、基本、詳細、指定なし: から一つのみ選択*]
・指定なし

[割付: *上記以外の個別に定義した監査対象事象*]
なし

FAU_GEN.1.2[E]

OSは、各監査記録において少なくとも以下の情報を記録しなければならない:
※下線部は詳細化。

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗); 及び

b) 各監査事象種別に対して、PP/STの機能コンポーネントの監査対象事象の定義に基づいた、[割付: *その他の監査関連情報*]

[割付: *その他の監査関連情報*]
なし

依存性: FPT_STM.1 高信頼タイムスタンプ

FAU_SAR.1[E]　監査レビュー

下位階層：なし

FAU_SAR.1.1[E]

IT環境は、[割付：*許可利用者*]が、[割付：*監査情報のリスト*]を監査記録から読み出せるようにしなければならない。

※下線部は詳細化。

[割付：*許可利用者*]

・システム管理者

[割付：*監査情報のリスト*]

監査ログファイルから以下の情報を読み出すことを可能とする。

・日付・時刻

・事象種別

・サブジェクト識別情報

・事象の結果

FAU_STG.1.2[E]

OSは、監査証跡内の格納された監査記録への不正な改変を[選択：*防止、検出：から一つのみ選択*]できねばならない。

※下線部は詳細化。

[選択：*防止、検出：から一つのみ選択*]

防止

依存性：FAU_GEN.1 監査データ生成

FAU_STG.1[E] 保護された監査証跡格納

下位階層: なし

FAU_STG.1.1[E]

OSは、格納された監査記録を不正な削除から保護しなければならない。

※下線部は詳細化。

FAU_STG.1.2[E]

OSは、監査証跡内の格納された監査記録への不正な改変を[選択: *防止、検出: から一つのみ選択*]できねばならない。

※下線部は詳細化。

[選択: *防止、検出: から一つのみ選択*]

防止

依存性: FAU_GEN.1 監査データ生成

FIA_UAU.2[E] アクション前の利用者認証

下位階層： FIA_UAU.1

FIA_UAU.2.1[E]

OSは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

※下線部は詳細化。

依存性： FIA_UID.1 識別のタイミング

FIA_UID.2[E] アクション前の利用者識別

下位階層： FIA_UID.1

FIA_UID.2.1[E]

OSは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

※下線部は詳細化。

依存性： なし

FIA_ATD.1[E] 利用者属性定義

下位階層: なし

FIA_ATD.1.1[E]

OSは、個々の利用者に属する以下のセキュリティ属性のリスト[割付:*セキュリティ属性のリスト*]を維持しなければならない。

※下線部は詳細化。

[割付:*セキュリティ属性のリスト*]

- OSユーザ名
- 権限属性

依存性: なし

FIA_USB.1[E] 利用者・サブジェクトの結合

下位階層：なし

FIA_USB.1.1[E]

OSは、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない:[割付: *利用者セキュリティ属性のリスト*]

※下線部は詳細化

[割付: *利用者セキュリティ属性のリスト*]

・OS ユーザ名

・権限属性

FIA_USB.1.2[E]

OSは、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない:［割付: *属性の最初の関連付けに関する規則*]

※下線部は詳細化

[割付: *属性の最初の関連付けに関する規則*]

・なし

FIA_USB.1.3[E]

OSは、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない:［割付: *属性の変更に関する規則*]

※下線部は詳細化

[割付: *属性の変更に関する規則*]

・なし

依存性：FIA_ATD.1 利用者属性定義

FPT_STM.1[E] 高信頼タイムスタンプ

下位階層: なし

FPT_STM.1.1[E]

OSは、OSおよびTSF自身の使用のために、高信頼タイムスタンプを提供できなければならない。

※下線部は詳細化

依存性: なし

6 TOE要約仕様

本章では、TOE セキュリティ機能の要件仕様を記述する。

6.1 TOEセキュリティ機能

本節では、TOE のセキュリティ機能を説明する。

表 6-1示したとおり、本節で説明するセキュリティ機能は、“第 5 章 TOEセキュリティ機能要件”に示したセキュリティ機能要件を満たす。

表 6-1　TOE 要約仕様と TOE セキュリティ機能要件の対応

TOE 要約仕様 / セキュリティ機能要件	アクセス制御機能	監査ログ出力機能	パスワード保護機能
FAU_GEN.1		○	
FAU_STG.3		○	
FDP_ACC.1	○		
FDP_ACF.1	○		
FMT_MOF.1		○	
FMT_MSA.1	○		
FMT_MSA.3	○		
FMT_MTD.1		○	
FMT_SMF.1	○	○	
FMT_SMR.1	○	○	
FPT_ITT.1			○
FPT_RVM.1	○	○	○
FPT_SEP.1	○	○	○

6.1.1 アクセス制御機能

本機能は、以下のセキュリティ機能群を有する。

[保護資産の分割ポリシー]

自動運転用定義情報は、所有者毎に作成される「プロジェクト」という単位で分割管理される。プロジェクト配下には、グループ（ジョブネットの集合)、ジョブネット（ジョブの集合)、ジョブが記載される。そのため以下では、アクセス制御機能の規定を、プロジェクト、グループ、ジョブネット、ジョブの用語を使用して行なう。

アクセス権限は、プロジェクト単位で設定が可能である。プロジェクトにはグループ/ジョブネット/ジョブを含む。設定可能な権限には、参照のみを行う「参照権」、参照およびジョブの操作を行う「操作権」、参照、操作、および更新を行う「更新権」、参照および更新を行う「登録権」がある。

プロジェクト(自動運転用定義情報)とアクセス権の関係イメージを図 6-1に示す。

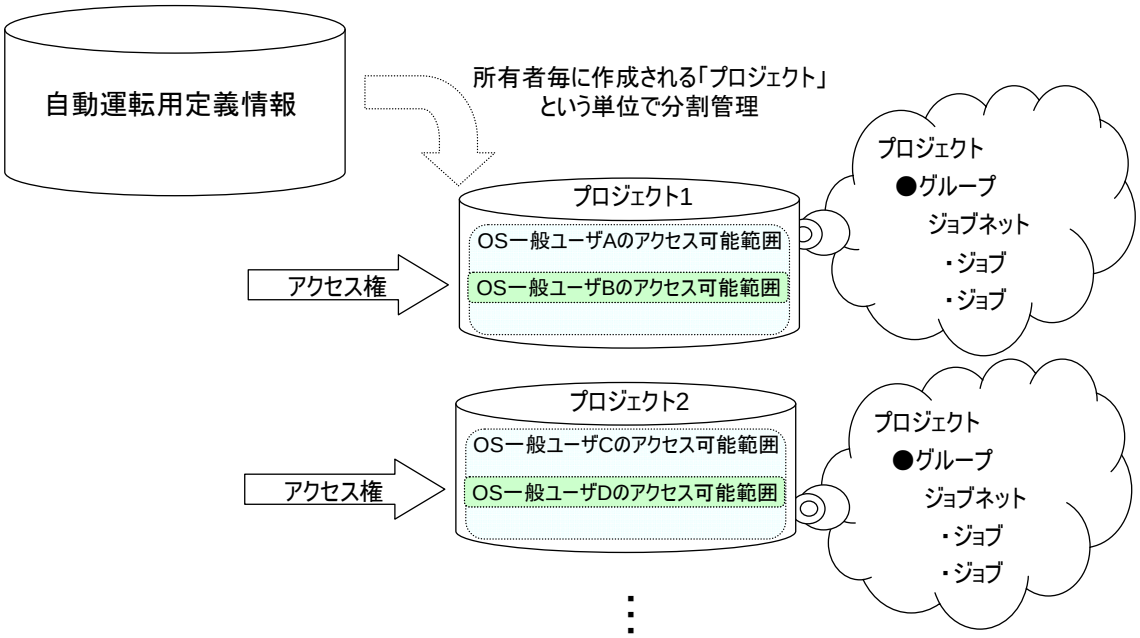

図 6-1 プロジェクト(自動運転用定義情報)とアクセス権の関係

[図の説明]

自動運転表定義情報は、所有者毎に作成されるプロジェクトという名称単位で分割管理される。プロジェクト配下には、グループ、ジョブネット、ジョブが存在する。プロジェクト毎に OS 一般ユーザのアクセス権が設定され、アクセス権に従い OS 一般ユーザは許可された範囲でアクセスが可能となる。

■アクセス制御機能の本体部

本機能は、OS ユーザに対し、プロジェクト、グループ、ジョブネット、ジョブへの許可された範囲内でのアクセスを制御する機能である。

OS一般ユーザに対するアクセス制御の規則を表 6-2に示す。(但し、ジョブを実行するためには、ジョブ所有者情報の定義にジョブの実行ユーザとして許可されたOSユーザ名が設定されている必要がある。)

表 6-2　OS 一般ユーザに対するアクセス制御規則

アクセス制御規則
プロジェクトの所有者ではないOS一般ユーザが、対象とするプロジェクト／グループ／ジョブネット／ジョブにアクセスする場合、OS一般ユーザのOSユーザ名が当該プロジェクトのアクセス制御情報に規定されているかの確認が行なわれ、規定されている場合、同アクセス制御情報に規定されている操作（登録、更新、操作、参照）が許可される。 ※グループ／ジョブネット／ジョブに対するアクセス権は、プロジェクトに対するアクセス権が継承される。

表 6-3に、プロジェクトの所有者、システム管理者に適用されるアクセス規則を示す。

表 6-3　プロジェクトの所有者、システム管理者に適用されるアクセス規則

明示的にアクセス許可する規則
プロジェクトの所有者が、所有するプロジェクト、グループ、またはジョブネット／ジョブにアクセスする場合、すべての操作（登録、更新、操作、参照）が許可される。
システム管理者が、すべてのプロジェクト、グループ、またはジョブネット／ジョブにアクセスする場合、すべての操作（登録、更新、操作、参照）が許可される。

■アクセス制御機能に関する管理機能部

本機能は、アクセス制御機能を管理するために利用する機能である。

システム管理者のみに提供された、アクセス制御機能に関わる設定機能を以下に示す。

- OS 一般ユーザに対する、プロジェクト（ひいては、グループ、ジョブネット／ジョブ）に対する操作範囲の設定（登録/変更/削除）
- プロジェクトの所有者の設定（登録/変更）
- 自動運転用定義情報の作成時にデフォルトで適用されるアクセス権限の変更（※）

（※）自動運転用定義情報を作成した際、デフォルトで適用されるアクセス権はすべての利用者のアクセス許可である。

[OS 一般ユーザのアクセス権設定単位]

本TOEでは、システム管理者による、OS一般ユーザに対する操作範囲の設定を簡単化するために、表 6-4に示す「設定ロール」単位で操作可能範囲を設定する機能を提供している。設定ロールの内訳を以下に示す。OS一般ユーザがプロジェクトの所有者の場合、更新権をもつOS一般ユーザと同じ権限を有することになる。

表 6-4　ロールと適用される操作の対応

設定ロール	単位	設定ロールに従い可能となる操作
更新権をもつ OS 一般ユーザ	プロジェクト	・プロジェクトの参照
	グループ	・グループの登録/更新/操作/参照
	ジョブネット /ジョブ	・ジョブネット/ジョブへの登録/更新/操作/参照
登録権をもつ OS 一般ユーザ	プロジェクト	該当操作なし
	グループ	・グループの登録/更新/参照
	ジョブネット /ジョブ	・ジョブネット/ジョブの登録/更新/参照
操作権をもつ OS 一般ユーザ	プロジェクト	・プロジェクトの参照
	グループ	・グループの操作/参照
	ジョブネット/ジョブ	・ジョブネット/ジョブの操作/参照
参照権をもつ OS 一般ユーザ	プロジェクト	・プロジェクトの参照
	グループ	・グループの参照
	ジョブネット/ジョブ	・ジョブネット/ジョブの参照

なお、本機能は、OS の識別認証の後に実行し、かつ、他のパスがないことから、迂回されることなく必ず実行する。

また、本機能は、不正な入力に伴う、プロセスの干渉による改ざんが行われないような実装にする。

6.1.2 監査ログ出力機能

本機能は、以下のセキュリティ機能群を有する。

■監査ログの収集

本機能では、本 TOE のセキュリティ機能である「アクセス制御機能」に関連する操作で発生する事象を監査ログファイルとして出力する機能を提供する。

表 6-5 監査イベントに本機能にて記録される事象を示す。

なお、表において、監査イベントの出力先(表では「出力先」と表記)が「監査ログファイル」である場合、以下の情報が監査イベントに含まれて採取される。

・「日付および時刻」(時刻については、ミリ秒単位)
・「操作者」
・「操作対象」(対象となるプロジェクト名等)
・「操作内容」(監査イベントの内容)
・「実行結果」(事象の成功／失敗)

表 6-5 監査イベント

監査の対象となるセキュリティ機能	監査イベント	出力先
アクセス制御機能	・プロジェクトのアクセス実行における成功事象（参照は除く）	監査ログファイル
	・グループののアクセス実行における成功事象（参照は除く）	
	・ジョブネットのアクセス実行における成功事象（参照は除く）	
	・ジョブのアクセス実行における成功事象（参照は除く）	
	・アクセス制御の管理機能部の利用事象 （具体的には以下） － 自動運転用定義情報の作成時にデフォルトで適用されるアクセス権限の変更 －OS 一般ユーザに対する、プロジェクトに対する操作範囲の設定（登録/変更/削除） －OS 一般ユーザに対する、プロジェクトの所有者の設定（登録/変更）	

なお、監査ログ出力機能の起動・終了事象は、イベントログにより採取されるため、TOEとしてはログ採取しない。

■ 監査ログ出力機能に関する管理機能部

本機能は、監査ログ出力機能を停止・起動するインタフェースを、システム管理者のみに提供する。

■ 監査ログファイルの有効期限

監査ログファイルの有効期限を変更する機能を、システム管理者のみに提供する。なお、有効期限を越えた場合、古い日付の監査ログファイルを削除する。

なお、事象の発生時、必ず監査ログファイルの生成が行われる。また、日付が変更された時点で、有効期限が切れた監査ログファイルを必ず削除する。

また、本機能は、不正な入力に伴う、プロセスの干渉による改ざんが行われないような実装にする。

6.1.3 パスワード保護機能

本機能は、内部ネットワーク上に流れるパスワードを、送信ごとに異なるデータに変換することで、暴露から保護する機能を提供する。

なお、本機能は、パスワード送信時に必ず実行する。

また、本機能は、不正な入力に伴う、プロセスの干渉による改ざんが行われないような実装にする。

6.2 セキュリティ機能強度

本 TOE の保証レベルが EAL1 ということから、AVA_SOF.1 が含まれないため、確率的または順列的メカニズムによって実現されている IT セキュリティ機能は識別せず、また、IT セキュリティ機能に対する機能強度の主張もしない。

6.3 保証手段

保証クラスに対する保証手段を表 6-6に示す。

表 6-6 保証要件と保証手段の対応

クラス	コンポーネント名	保証手段
構成管理	ACM_CAP.1	TOE バージョンの表示
配付と運用	ADO_IGS.1	Systemwalker Operation Manager セキュリティガイド Systemwalker Operation Manager 解説書 (注) Systemwalker Operation Manager 導入手引書 (注)
開発	ADV_FSP.1	Systemwalker Operation Manager V13.2.0 セキュリティ機能仕様書
	ADV_RCR.1	Systemwalker Operation Manager V13.2.0 表現対応表
ガイダンス	AGD_ADM.1 AGD_USR.1	Systemwalker Operation Manager セキュリティガイド Systemwalker Operation Manager 解説書 (注) Systemwalker Operation Manager 導入手引書 (注) Systemwalker Operation Manager 使用手引書 (注) Systemwalker Operation Manager リファレンスマニュアル (注) Systemwalker Operation Manager メッセージ説明書 (注) Systemwalker Operation Manager トラブルシューティングガイド (注) Systemwalker Operation Manager スケジュール分散機能説明書 (注)
テスト	ATE_IND.1	TOE

(注) 表中では、「- UNIX/Windows(R)共通 -」の記載を省略する。

7 PP主張

本 ST が適合する PP は存在しない。

8 根拠

8.1 セキュリティ対策方針根拠

TOE セキュリティ環境に対応するセキュリティ対策方針の関係を表 8.1 に示す。

表 8-1　TOE セキュリティ環境とセキュリティ対策方針の対応

TOE セキュリティ環境 / セキュリティ対策方針	T. PASSWORD_TAP	T. UAUSER_CLIENT	T. UAUSER_COMMAND	T. UAACTION	A. ADMIN	A. PASSWORD	A. PLACE	A. NETWORK	A. OS_ACCESS
O. PW_PROTECT	○								
O. PERMIT_USE				○					
OE. OS_I&A		○	○						
OE. OS_AUDIT				○					
OE. AUDIT				○					
OE. ATTRIBUTE				○					
OE. ASSIGN					○				
OE. PASSWORD						○			
OE. PLACE							○		
OE. NETWORK								○	
OE. OS_SETUP									○
OE. COMMAND_ACCESS	○								

以下に、『表 8-1 TOEセキュリティ環境とセキュリティ対策方針の対応』の根拠を示す。

前提条件

A. ADMIN

A. ADMIN は、システム管理者が不正な操作を行わない信頼できる人物であることを規定した前提条件である。

この前提条件は、システム管理者として信頼できる人物を選任すると共に、当該人物に対し教育を行なうことで実現できる。

OE. ASSIGN において、以下の項目を規定している。

・組織の責任者が、システム管理者として信頼できる人物を選任すると共に、不正を行なわないよう教育を行なう。

従って、セキュリティ対策方針 OE.ASSIGN が満たされることにより、本前提条件を実現することができる。

A.PASSWORD

A.PASSWORD は、パスワードの管理について、以下を想定した前提条件である。

・TOE を利用する OS 一般ユーザのパスワードは、システム管理者及び本人以外に知られないように管理される。

この前提条件は、パスワードの管理を適切に行なうことで実現できる。

OE.PASSWORD において、パスワードの管理について、以下の項目を規定している。

・システム管理者は、TOE を利用する OS 一般ユーザに対し、自身のパスワードを他に漏洩しないように管理する事を教育し、遵守させなければならない。

従って、セキュリティ対策方針 OE.PASSWORD が満たされることにより、本前提条件を実現することができる。

A.PLACE

A.PLACE は、本 TOE が動作するサーバが、システム管理者以外が入退出できない、事務フロアやサーバルーム等に設置されることを想定した前提条件である。

この前提条件は、本 TOE が動作するサーバを、システム管理者以外が容易に入室不可能な事務フロアやサーバルーム等に設置することで実現できる。

OE.PLACE において、システム管理者が、本 TOE が動作するサーバを、人的、機械的又は電子的な手段による入退出管理が施された、システム管理者以外が容易に入室不可能な事務フロアやサーバルーム等に設置することを規定している。

従って、セキュリティ対策方針 OE.PLACE が満たされることにより、本前提条件を実現することができる。

A.NETWORK

A.NETWORK は、外部ネットワークから TOE にアクセスし、不正を行なわれないようにするため、TOE が外部ネットワークから直接アクセスされないイントラネット環境にて動作されることを想定した前提条件である。

この前提条件は、本 TOE が動作するサーバ、クライアントを外部ネットワークから直接アクセスできない、イントラネット内に接続することで実現できる。

OE.NETWORK において、システム管理者が、本 TOE が動作するサーバ、クライアントをネットワークに接続する場合、ファイアウォール等で区切られたイントラネット内に接続することを規定している。

従って、セキュリティ対策方針 OE.NETWORK が満たされることにより、本前提条件を実現することができる。

A.OS_ACCESS

A.OS_ACCESS は、TOE を介さず、直接 OS から TOE で扱う資源にアクセスできないよう、アクセス権設定されることを想定した前提条件である。

この前提条件は、TOE を介さず、直接サーバ上の OS から TOE で扱う資源に不正されないように、OS のアクセス権設定を行なうことで実現できる。

OE.OS_SETUP により、システム管理者が、本 TOE を介さず、直接 OS から TOE で扱う資源に対して不正できないように、OS のアクセス権設定を行うことが規定されている。

従って、セキュリティ対策方針 OE.OS_SETUP が満たされることにより、本前提条件を実現することができる。

脅威

T.PASSWORD_TAP

T.PASSWORD_TAP は、悪意のある者が、内部ネットワーク上に流れるパスワードを盗聴し、内容を暴露する脅威である。

この脅威に対抗するためには、本 TOE は、クライアント機能およびコマンドを使用した際に内部ネットワーク上に流れるパスワードの内容を解析できないようにすることで実現できる。

内部ネットワーク上に流れるパスワードに関しては、TOE では、O.PW_PROTECT により、クライアント機能を使用時に、内部ネットワーク上に流れるパスワードの内容を解析できないようにすることを規定している。また、OE.COMMAND_ACCESS により、システム管理者及び OS 一般ユーザが、コマンドを使用時に、悪意のあるものに内部ネットワーク上に流れるパスワードが解析されないように、SSH を利用することが規定されている。

従って、セキュリティ対策方針 O.PW_PROTECT、OE.COMMAND_ACCESS が満たされることにより、本脅威に対抗することができる。

T.UAUSER_CLIENT

T.UAUSER_CLIENT は、悪意のある者が、クライアント機能を使用して、システム管理者、及び OS 一般ユーザになりすまし、自動運転用定義情報の改ざんを行い、ジョブの計画的な実行を阻害する脅威である。

この脅威に対抗するためには、クライアント機能を使用したシステム管理者及び OS 一般ユーザを識別し、本人であることを確認することで実現できる。

OE_OS_I&A により、クライアント機能を使用したシステム管理者及び OS 一般ユーザを確認するために識別と認証を行い、識別と認証が失敗した場合には、TOE の利用を拒否す

ることを規定している。
従って、セキュリティ対策方針 OE.OS_I&A が満たされることにより、本脅威に対抗することができる。

T.UAUSER_COMMAND

T.UAUSER_COMMAND は、悪意のある者が、コマンドを使用して、システム管理者及び OS 一般ユーザになりすまし、自動運転用定義情報の改ざんを行い、ジョブの計画的な実行を阻害する脅威である。
この脅威に対抗するためには、コマンドを使用したシステム管理者、OS 一般ユーザを識別し、本人であることを確認することで実現できる。
OE_OS_I&A により、コマンドを使用したシステム管理者及び OS 一般ユーザを確認するために識別と認証を行い、識別と認証が失敗した場合には、TOE の利用を拒否することを規定している。
従って、セキュリティ対策方針 OE.OS_I&A が満たされることにより、本脅威に対抗することができる。

T.UAACTION

T.UAACTION は、OS 一般ユーザとして識別認証されたものがクライアント機能またはコマンドを使用して、許可された範囲を超えて操作を行い、自動運転用定義情報を改ざんする脅威である。
この脅威に対抗するためには、OS 一般ユーザが、許可された担当業務の範囲内でのみ、自動運転用定義情報への操作を許可することで実現できる。
TOE では、O.PERMIT_USE により、システム管理者が許可した範囲のみ、OS 一般ユーザが操作できるようにし、許可された範囲以外の操作を行おうとした場合は、その操作を拒否することを規定している。
また、OE.ATTRIBUTE により、OS は、TOE が行う OS 一般ユーザに対する許可された範囲での自動運転用定義情報への操作制限（O.PERMIT_USE）をサポートする目的で、OS 一般ユーザと利用者プロセスとの結合を行う。
OE.AUDIT により、本対策方針で示した「不正な兆候がないことを確認するためのログ」を閲覧する機能、及び監査ログファイルを保護する機能を提供するため、許可範囲での制限に対する不正な兆候がないことを監査でき、かつ監査ログファイルが保護される。なお、この際、監査ログには、監査の開始と終了の事象が採取されないため、OE.OS_AUDIT により、OS は TOE の監査ログ出力機能の起動と終了の事象を採取する機能を提供する。また、本対策方針により、OS は監査ログに使用する時刻を提供する。
従って、セキュリティ対策方針 O.PERMIT_USE、OE.AUDIT、OE.OS_AUDIT が満たされることにより、本脅威に対抗することができる。

8.2 セキュリティ要件根拠

8.2.1 セキュリティ機能要件根拠

セキュリティ対策方針に対するセキュリティ機能要件の対応を表8.2に示す。

表 8-2　セキュリティ対策方針とセキュリティ機能要件の対応

セキュリティ機能要件 ＼ セキュリティ対策方針	O.PW_PROTECT	O.PERMIT_USE	OE.OS_I&A	OE_OS_AUDIT	OE.AUDIT	OE.ATTRIBUTE
FAU_GEN.1		○				
FAU_STG.3		○				
FDP_ACC.1		○				
FDP_ACF.1		○				
FMT_MOF.1		○				
FMT_MSA.1		○				
FMT_MSA.3		○				
FMT_MTD.1		○				
FMT_SMF.1		○				
FMT_SMR.1		○				
FPT_ITT.1	○					
FPT_RVM.1	○	○				
FPT_SEP.1	○	○				
FAU_GEN.1[E]				○		
FAU_SAR.1[E]					○	
FAU_STG.1[E]					○	
FIA_UAU.2[E]			○			
FIA_UID.2[E]			○			
FIA_ATD.1[E]						○
FIA_USB.1[E]						○
FPT_STM.1[E]				○		

以下に、『表 8-2セキュリティ対策方針とセキュリティ機能要件の対応』の根拠を示す。

O.PW_PROTECT

O.PW_PROTECT は、内部ネットワーク上に流れるパスワードの内容を解析できないようにする対策方針である。

本対策方針を実現するためには、解析できないようにすることの目的が暴露からの保護であることから、内部ネットワーク上に流れるパスワードを暴露から保護するための機能要件を導出する必要がある。

そのため、本 TOE では以下の機能要件を導出する。

・FPT_ITT.1 により、パスワードが TOE の別々のパーツ間で送られる場合、パスワードを暴露から保護する

また、以下により、本対策方針に関わる機能要件の確実な実施が保証される。

・FPT_RVM.1 により、本対策方針に関わる機能要件は確実に実施され、成功することを保証する。

・FPT_SEP.1 により、本体策方針に関わる機能要件は、信頼できないサブジェクトからの干渉や改ざんから保護されることを保証する。

以上のセキュリティ機能要件によって、O.PW_PROTECT を満たすことができる。

O.PERMIT_USE

O.PERMIT_USE は、システム管理者が許可した範囲のみ、OS 一般ユーザが操作できるようにし、許可された範囲以外の操作を行おうとした場合は、その操作を拒否する対策方針である。

本対策方針を実現するためには、利用者を代行する利用者プロセスに対し、システム管理者が許可したアクセスのみを許可するアクセス制御を行なう機能要件を導出する必要がある。

そのため、本 TOE では以下の機能要件を導出する。

・FDP_ACC.1 により、利用者プロセスと自動運転用定義情報間において、システム管理者が許可したアクセスのみを許可する「自動運転用定義情報アクセス制御 SFP」を定義し、FDP_ACF.1 により当該アクセス制御 SFP の具体的なアクセス制御規則を規定する。

また、本対策方針に関わる機能要件を管理するために、以下の機能要件を導出する。

・FMT_MSA.1 により、アクセス制御 SFP に関係する属性を管理する能力を、許可された識別された役割のみに制限する。(本要件と、FMT_SMF.1 により、システム管理者が許可するアクセスの規定が行なわれる。)

・FMT_MSA.3 により、生成時許可的デフォルト値が与えられるオブジェクト（自動運転用定義情報）について、そのデフォルト値を上書きする代替の初期値を指定することをシステム管理者だけに制限する。

・FMT_SMF.1 により、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1 の実体となる、セキュリティ管理機能を提供する。

・FMT_SMR.1 により、アクセス制御機能に関係した、許可された識別された役割の維持や、利用者との関連付けが行なわれる。

・FMT_MOF.1 により、監査ログ出力機能を起動・停止する能力をシステム管理者のみに提供する。

・FMT_MTD.1 により、監査ログファイルに対する有効期限を設定する能力をシステム管理者のみに提供する。

また本対策方針に関わる機能要件が確実に動作していることを監査できるようにするために、以下の機能要件を導出する。

・FAU_GEN.1 により、アクセス制御に関わる機能要件に対する操作の監査ログが採取される。なお、FAU_GEN.1 における監査レベルは「最小」を選択する。これは、本対策方針において監査に期待する項目は以下であり、これらの項目は、監査レベル「最小」で満たされることによる。

- アクセス制御の機能が有効に動作し、オブジェクトに対する操作制御が正しく行われているかを確認できるようにする。そのために、アクセス制御の成功事象を採取する。
- アクセス制御に対する管理の機能が不正に使用され、アクセス制御の機能が無効化されていないか確認できるようにする。そのために、アクセス制御に対する管理の機能の使用事象を採取する。

・FAU_STG.3 により、旧監査ログを廃棄することにより監査ログファイル格納域を確保し、新監査ログを記録することを保護する。

また、以下により、本対策方針に関わる機能要件の確実な実施が保証される。

・FPT_RVM.1 により、本対策方針に関わる機能要件は確実に実施され、成功することを保証する。

・FPT_SEP.1 により、本体策方針に関わる機能要件は、信頼できないサブジェクトからの干渉や改ざんから保護されることを保証する。

以上のセキュリティ機能要件によって、O.PERMIT_USE を満たすことができる。

OE.OS_I&A

OE.OS_I&A は、IT 環境である OS がシステム管理者または OS 一般ユーザを識別認証し、識別と認証が失敗した場合に、TOE の利用を拒否する対策方針である。

本対策方針を実現するためには、正当なシステム管理者、OS 一般ユーザであることを確認する識別認証の機能要件を導出する必要がある。そのため、IT 環境では、以下の機能要件を導出する。

・FIA_UAU.2[E]及び FIA_UID.2[E]により、TOE の利用の前に識別認証を行なう。

以上のセキュリティ機能要件によって、OE.OS_I&A を満たすことができる。

OE.OS_AUDIT

OE.OS_AUDIT は、OS が TOE の監査ログ出力機能の起動と終了の事象を採取する機能を提供し、また、監査ログのために時刻を提供する対策方針である。

本対策方針を実現するためには、TOE の監査ログ出力機能の起動と終了の事象の監査記録を生成する機能要件、および時刻を提供する機能要件を導出する必要がある。

そのため、IT 環境では、以下の機能要件を導出する。

・ FAU_GEN.1[E]により、OS は TOE の監査機能の起動と終了の事象の監査記録を生成する。

・ FPT_STM.1[E]により、OS は時刻を提供する。

以上のセキュリティ機能要件によって、OE.OS_AUDIT を満たすことができる。

OE.AUDIT

OE.AUDIT は、IT 環境が、本 TOE に対する不正な兆候がないかを確認するための監査ログを閲覧する機能、及び監査ログファイルを保護する機能を提供する対策方針である。

本対策方針を実現するためには、監査ログファイルを読みやすい形式で閲覧するための機能要件を導出する必要がある。また、監査記録の不正な削除の保護、監査記録の不正な改変を保護（これらは、監査ログファイルの保護に通じる）する機能要件を導出する必要がある。そのため、IT 環境では、以下の機能要件を導出する。

・FAU_SAR.1[E]により、システム管理者に、見やすい形式で監査ログファイルを閲覧する機能を提供する。

・FAU_STG.1[E]により、格納された監査記録を不正な削除から保護し、監査証跡内の格納された監査記録への不正な改変を防止する機能を提供する

以上のセキュリティ機能要件によって、OE.AUDIT を満たすことができる。

OE.ATTRIBUTE

OS は、TOE が行う OS 一般ユーザに対する許可された範囲での自動運転用定義情報への操作制限をサポートする目的で、OS 一般ユーザと利用者プロセスとの結合を行う対策方針である。

本対策方針を実現するためには、セキュリティ属性を、利用者を代行するサブジェクト（プロセス）に関連付ける機能要件と、利用者に属するセキュリティ属性のリストを維持する機能要件を導出する必要がある。そのため、IT 環境では、以下の機能要件を導出する。

・FIA_ATD.1[E]により、利用者に属するセキュリティ属性の定義が行なわれ、FIA_USB.1[E]により、定義されたセキュリティ属性と利用者を代行する利用者プロセスとの結合を行なう。

以上のセキュリティ機能要件によって、OE.ATTRIBUTE を満たすことができる。

8.2.2 TOEセキュリティ機能要件間の依存関係

セキュリティ機能要件の依存関係を表 8-3に示す。なお、依存関係に対して問題がないことの根拠を表中の「問題がないことの根拠」に示す。

表 8-3　コンポーネントの依存関係

コンポーネント	依存関係	問題がないことの根拠
FAU_GEN.1	FPT_STM.1[E]	すべての依存関係を満たす。
FAU_STG.3	FAU_STG.1[E]	すべての依存関係を満たす
FDP_ACC.1	FDP_ACF.1	すべての依存関係を満たす。
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	すべての依存関係を満たす。
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	すべての依存関係を満たしている。
FMT_MSA.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	すべての依存関係を満たしている。
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	すべての依存関係を満たしている。
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	すべての依存関係を満たしている。
FMT_SMF.1	なし	－
FMT_SMR.1	FIA_UID.2[E]	本来の依存関係はFIA_UID.1であるが、FIA_UID.2はその上位コンポーネントである。
FPT_ITT.1	なし	－
FPT_RVM.1	なし	－
FPT_SEP.1	なし	－
FAU_GEN.1[E]	FPT_STM.1[E]	すべての依存関係を満たす。
FAU_SAR.1[E]	FAU_GEN.1 FAU_GEN.1[E]	すべての依存関係を満たす。
FAU_STG.1[E]	FAU_GEN.1 FAU_GEN.1[E]	すべての依存関係を満たす
FIA_UAU.2[E]	FIA_UID.2[E]	本来の依存関係はFIA_UID.1であるが、FIA_UID.2はその上位コンポーネントである。
FIA_UID.2[E]	なし	－
FIA_ATD.1[E]	なし	－

コンポーネント	依存関係	問題がないことの根拠
FIA_USB.1[E]	FIA_ATD.1[E]	すべての依存関係を満たしている。
FPT_STM.1[E]	なし	－

8.2.3 TOEセキュリティ機能要件の相互作用

[セキュリティ機能要件のセットが内部的に一貫する理由]

8.2.2に示したように、セキュリティ機能要件は一部の例外を除き、それぞれと依存関係のあるセキュリティ機能要件およびそれらの操作を満たし、相互補完している。また、機能要件間で、互いに矛盾した動作を行う機能要件や操作はない。そのため、セキュリティ機能要件のセットは内部的に一貫している。

明示的な依存関係は要求されないが、相互支援を目的として選択されたセキュリティ機能要件を『表8-4 TOEセキュリティ機能要件の相互作用について』に示す。

表8-4 TOEセキュリティ機能要件の相互作用について

機能要件	相互サポート			
	迂回防止	非活性化	改ざん防止	無効化検出
FAU_GEN.1	FPT_RVM.1	FMT_MOF.1	FPT_SEP.1	N/A
FAU_STG.3	FPT_RVM.1	FMT_MOF.1	FPT_SEP.1 FMT_MTD.1	N/A
FDP_ACC.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FDP_ACF.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FMT_MOF.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FMT_MSA.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FMT_MSA.3	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FMT_MTD.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FMT_SMF.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FMT_SMR.1	FPT_RVM.1	N/A	FPT_SEP.1	不要
FPT_ITT.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FPT_RVM.1	N/A	N/A	N/A	N/A
FPT_SEP.1	N/A	N/A	N/A	N/A

N/A:適用外（機能要件の「監査」にない、または、自分自身をさしている項目。非活性化に関しては、非活性化させる管理機能がない項目。また、無効化検出に関しては、「基本」以上の項目(本TOEでは、「最小」を選択しているため)）

不要：本来は保証対象であるが、本TOE固有の理由で保証する必要がない項目

FPT_RVM.1<迂回防止>

TOE を利用する際には、OS による識別認証(FIA_UAU.2[E]、FIA_UID.2[E])が動作し、その後にアクセス制御に関係する機能要件（FDP_ACC.1、FDP_ACF.1）が必ず動作しかつ、他のパスがないため、間接的に FPT_RVM.1 による迂回防止がなされている。

また､FPT_ITT.1 については､クライアント機能を使用したパスワードの送付の際には、通信に必ず介在する(逆に本機能要件が停止した状態では、通信は行なわれない）ため、FPT_RVM.1 による迂回防止がなされる。

また、FAU_GEN.1 については、FPT_RVM.1 により、事象の発生時、必ず監査記録の生成が行われる。FAU_STG.3 については、FPT_RVM.1 により、日付が変更された時点で、有効期限が切れた監査ログファイルを必ず削除する。

また、FMT_MOF.1、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1、FMT_SMF.1 および FMT_SMR.1 も同様に、セキュリティ機能のふるまいやセキュリティ属性および役割が維持され、FPT_RVM.1 による迂回防止がなされる。

従って、FPT_RVM.1 により、関係する機能要件に対する迂回防止を支援している。

FMT_MOF.1<非活性化>

FMT_MOF.1 により、監査ログ出力機能に関するセキュリティ機能要件を非活性化させる管理機能の利用を、システム管理者のみに制限しているため、TOE を非活性化させる攻撃へ対抗している。

従って、FMT_MOF.1 により、関係する機能要件への非活性化防止を支援している。

改ざん防止

・TSF データの改ざん防止<FMT_MTD.1>

FMT_MTD.1 により監査ログファイルの有効期限の改変を、システム管理者のみに制限しているため、TSF データの改ざん(延いては、TSF のふるまい変更)する攻撃へ対抗している。

[不要の理由]

監査ログファイルの有効期限以外には TSF データはないため、他のセキュリティ機能要件への TSF データの改ざん防止は不要である。

・FPT_SEP.1<サブジェクトの干渉による、改ざん防止>

本 TOE は、OS 上で動作する製品であるため、他の不正なサブジェクト（アプリケーション等）との干渉は、OS が提供する仮想空間の管理機能により防止される。

また、FPT_SEP.1 により、不正な入力に伴う、サブジェクトの干渉や改ざんのインタフェースが実装されないことが保証される。

従って、FPT_SEP.1 により、関係する機能要件に対するサブジェクトの干渉による改ざ

ん防止を支援している。

FAU_GEN.1<無効化検出>

FAU_GEN.1により、TOEのセキュリティ機能要件の実行に伴い、セキュリティ関連事象を記録する。この関連事象の記録により、セキュリティ機能要件の無効化を狙った攻撃の検出を可能にする。

従って、FAU_GEN.1によって関係する機能要件の無効化防止を支援している。

[不要の理由]

FMT_SMR.1に関しては、役割の一部をなす利用者のグループに対する改変が行なえないため、監査対象に該当する事象が存在せず、監査ログを採取する必要はない。

8.2.4 最小機能強度根拠

TOE が利用される環境での攻撃者の攻撃能力を低レベルと定義しているため、攻撃方法は、公開インタフェース、公開情報を利用したものとなる。低レベルの攻撃であれば、TOE が実施している対策である O.PW_PROTECT、O.PERMIT_USE で対抗できるため、TOE のセキュリティ対策方針は低レベルの攻撃に対抗しているといえる。

従って、TOEのセキュリティ対策方針が低レベルの攻撃者に対抗しているため、TOEのセキュリティ対策方針は最小機能強度SOF-基本と一貫している。

8.2.5 セキュリティ保証要件根拠

TOE には、市場からの要求として、利用者にとって価値ある資産（保護資産）の保護に配慮されていることに対する、独立した第三者による保証が提供されていることが望まれている。そのため、TOE は仕様に対する独立テストや提供されるガイダンスの調査など、市場の要求を満たす第三者保証を得ることが求められる。

このような市場の要求に答えるための必要最小限の保証を得る評価保証レベルとして EAL1 は適している。

8.3 TOE要約仕様根拠

8.3.1 TOE要約仕様に対するセキュリティ機能要件の適合性

表 8-5　TOE 要約仕様に対するセキュリティ機能要件の適合性

TOE 要約仕様 / セキュリティ機能要件	アクセス制御機能	監査ログ出力機能	パスワード保護機能
FAU_GEN.1		○	
FAU_STG.3		○	
FDP_ACC.1	○		
FDP_ACF.1	○		
FMT_MOF.1		○	
FMT_MSA.1	○		
FMT_MSA.3	○		
FMT_MTD.1		○	
FMT_SMF.1	○	○	
FMT_SMR.1	○	○	
FPT_ITT.1			○
FPT_RVM.1	○	○	○
FPT_SEP.1	○	○	○
FAU_GEN.1[E]	IT 環境により実現される		
FAU_SAR.1[E]			
FAU_STG.1[E]			
FIA_UAU.2[E]			
FIA_UID.2[E]			
FIA_ATD.1[E]			
FIA_USB.1[E]			
FPT_STM.1[E]			

以下に、『表 8-5 TOE要約仕様とセキュリティ機能要件の対応』の根拠を示す。

[セキュリティ機能の組み合わせがセキュリティ機能要件を満たす理由]

セキュリティ機能要件が、複数のセキュリティ機能によって実現されるものについて、セキュリティ機能の組み合わせが、各セキュリティ機能のバイパス、改ざん、非活性化等のセキュリティの弱点を生じさせない理由を示す。

- FMT_SMF.1、FMT_SMR.1、FPT_RVM.1、FPT_SEP.1 について、対象とするエンティティが、セキュリティ機能毎にそれぞれ異なるため、セキュリティ機能要件を実現するために、一緒に動作はしない。

以下、それぞれの機能要件が実現されている根拠を示す。

FAU_GEN.1

本セキュリティ機能要件は、監査対象事象に対して、監査記録を取得可能であることを要求する。これに対して、セキュリティ機能「監査ログ出力機能」では、監査イベントとして本セキュリティ機能要件で定義した情報を取得し、監査ログファイルに出力する。なお、監査機能の起動・停止のログは、「監査ログ出力機能」ではなく、イベントログによって採取されるため、本セキュリティ機能要件で規定された監査事象は満たされる。

よって、本セキュリティ機能要件は満たされる。

FAU_STG.3

本セキュリティ要件は、事前に定義された限界を超えた場合の、監査ログファイルに対するアクションを実行することを要求する。これに対して、セキュリティ機能「監査ログ出力機能」では、有効期限を越えた場合、古い日付の監査ログファイルを削除する。

よって、本セキュリティ機能要件は満たされる。

FDP_ACC.1

本セキュリティ機能要件は、サブジェクト（利用者プロセス）、オブジェクト（自動運転用定義情報）およびサブジェクトとオブジェクト間の操作（参照、操作、更新、登録）のリストに対して、自動運転用定義情報アクセス制御 SFP を実施することを要求する。

これに対して、セキュリティ機能「アクセス制御機能」は、システム管理者および OS 一般ユーザを代行する利用者プロセスと、自動運転用定義情報の分割単位であるプロジェクト／グループ／ジョブネット／ジョブ間の操作（参照、操作、登録、更新）を制限する、アクセス制御を行なう。

よって、本セキュリティ機能要件は満たされる。

FDP_ACF.1

本セキュリティ機能要件は、セキュリティ属性によるアクセス制御の適用を要求する。これに対して、セキュリティ機能「アクセス制御機能」は、以下を提供する。

- OS 一般ユーザに適用するアクセス制御規則を規定する
- 明示的にアクセスを承認する規則として、プロジェクトの所有者、システム管理者に適用されるアクセス制御を規定する

なお FDP_ACF.1 での、利用者プロセス（サブジェクト）、OS ユーザ名、権限属性（それぞれ、サブジェクト属性）は、「アクセス制御機能」では、システム管理者、OS 一般ユーザに詳細化している。

また、自動運転用定義情報（オブジェクト）は、プロジェクト/グループ/ジョブネット/ジョブに詳細化し、また、所有者名、OS 一般ユーザに対するアクセス権（OS ユーザ名・アクセス権レベル）（それぞれオブジェクト属性）は、「アクセス制御機能」では、所有者名や、アクセス制御情報に規定されている操作、に詳細化している。

よって、本セキュリティ機能要件は満たされる。

FMT_MOF.1

本セキュリティ機能要件は、セキュリティ機能を動作・停止する能力を許可された役割のみに提供することを要求する。これに対して、セキュリティ機能「監査ログ出力機能」は、監査ログ出力機能を起動・停止するインタフェースをシステム管理者のみに提供する。よって、本セキュリティ機能要件は満たされる。

FMT_MSA.1

本セキュリティ機能要件は、自動運転用定義情報アクセス制御 SFP に関するセキュリティ属性の管理を許可された役割のみに制限することを要求する。本セキュリティ機能要件で規定している内容は、具体的には以下の通りである。

システム管理者のみに以下を行なう能力を制限する

① OS 一般ユーザに関係するオブジェクト属性(OS 一般ユーザのアクセス権)の登録・改変・削除

② 所有者名の登録・改変

これに対して、「アクセス制御機能」は、①の詳細化として、OS 一般ユーザに対する自動運転用定義情報の管理単位であるプロジェクト（ひいては、グループ、ジョブネット／ジョブ）に対するアクセス制御に関わる設定(登録/変更/削除)機能を、システム管理者のみに提供する。②の詳細化として、プロジェクトの所有者を設定(登録/変更)する機能を、システム管理者に提供する。

よって、本セキュリティ機能要件は満たされる。

FMT_MSA.3

本セキュリティ機能要件は、自動運転用定義情報アクセス制御 SFP を実施するために使われるセキュリティ属性として、許可的なデフォルト値を与えることを要求する。また、オブジェクトや情報が生成される際は、許可された役割の者がデフォルト値を上書きする代替の初期値を指定することを許可することを要求する。これに対して、セキュリティ機能「アクセス制御機能」は、自動運転用定義情報を作成する際、デフォルトで適用されるアクセス権（すべての利用者のアクセス許可）について規定している。

また、自動運転用定義情報を作成する際にデフォルトで適用されるアクセス権を変更する機能を、システム管理者のみに提供する。よって、本セキュリティ機能要件は満たされる。

FMT_MTD.1

本セキュリティ機能要件は、TSF データの管理を許可された役割の者のみに制限することを要求する。これに対して「監査ログ出力機能」では、監査ログファイルの有効期限を変更する能力をシステム管理者のみに提供する。よって、本セキュリティ機能要件は満たされる。

FMT_SMF.1

本セキュリティ機能要件は、セキュリティ管理機能の提供を要求する。これに対して、「アクセス制御機能」「監査ログ出力機能」は FMT_MOF.1、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1 にて示した許可利用者への制限機能の実体となる管理機能を提供している。よって、本セキュリティ機能要件は満たされる。

FMT_SMR.1

本セキュリティ機能要件は、許可された識別された役割を維持することを要求する。これに対して、「アクセス制御機能」「監査ログ出力機能」は、システム管理者の役割を維持管理する機能を提供する。よって、本セキュリティ機能要件は満たされる。

FPT_ITT.1

本セキュリティ機能要件は、パスワードが TOE の別々のパーツ間で送られる場合、パスワードを暴露から保護することを要求する。これに対して「パスワード保護機能」では、内部ネットワーク上に流れるパスワードを、送信ごとに異なるデータに変換することで、暴露から保護する機能を提供する。よって、本セキュリティ機能要件は満たされる。

FPT_RVM.1

本セキュリティ機能要件は、セキュリティ機能が必ず動作することを要求する。これに対して、「アクセス制御機能」「監査ログ出力機能」「パスワード保護機能」は操作を行う際に必ず実行する。よって、本セキュリティ機能要件は満たされる。

FPT_SEP.1

本セキュリティ機能要件は、セキュリティ機能の実行のため、信頼できないサブジェクトによる干渉と改ざんから保護することを要求する。これに対して、「アクセス制御機能」「監査ログ出力機能」「パスワード保護機能」は、干渉されることによって改ざんが行われないような実装にする。よって、本セキュリティ機能要件は満たされる。

8.3.2 セキュリティ機能強度根拠

本 TOE の保証レベルが EAL1 ということから、AVA_SOF.1 が含まれないため、明示された機能要件、および IT セキュリティ機能に対する機能強度主張をしていない。そのため、IT セキュリティ機能に対する機能強度主張が、TOE セキュリティ機能要件に対する機能強度と一貫している根拠を示す必要はない。

8.3.3 保証手段根拠

表 6-6に示した通り、全てのTOEセキュリティ保証要件は保証手段により示されたドキュメントのセットによって対応付けられる。

以下に、EAL1 の保証要件セットが各保証手段により満たされる根拠を示す。

ACM_CAP.1　　バージョン番号

【保証手段】

・TOE バージョンの表示

【保証要件根拠】

「TOE バージョンの表示」により、TOE の購入者に対し、TOE を一意にリファレンスする手段を提供する。そのため、保証要件 ACM_CAP.1 は満たされる。

ADO_IGS.1　　設置、生成、及び立上げ手順

【保証手段】

・Systemwalker Operation Manager セキュリティガイド

・Systemwalker Operation Manager 解説書 - UNIX/Windows(R)共通 -

・Systemwalker Operation Manager V13.2.0 導入手引書 - UNIX/Windows(R)共通 -

【保証要件根拠】

保証手段に示した資料には、TOE をセキュアな構成にするために採用される、設置手順、生成手順および起動の確認方法を規定する。そのため、保証要件 ADO_IGS.1 は満たされる。

ADV_FSP.1　　非形式的機能仕様

【保証手段】

・Systemwalker Operation Manager V13.2.0 セキュリティ機能仕様書

【保証要件根拠】

保証手段に示した資料には、セキュリティ機能とその外部インタフェースの仕様を規定する。そのため、保証要件 ADV_FSP.1 は満たされる。

ADV_RCR.1　　非形式的対応の実証

【保証手段】

・Systemwalker Operation Manager V13.2.0 表現対応表

【保証要件根拠】

保証手段である「Systemwalker Operation Manager V13.2.0 表現対応表」には、TOE のセキュリティ機能の各レベル（要約仕様－機能仕様）での完全な対応を記述する。

そのため、保証要件 ADV_RCR.1 は満たされる。

AGD_ADM.1　　管理者ガイダンス

【保証手段】

・Systemwalker Operation Manager セキュリティガイド
・Systemwalker Operation Manager　解説書 - UNIX/Windows(R)共通 -
・Systemwalker Operation Manager　導入手引書 - UNIX/Windows(R)共通 -
・Systemwalker Operation Manager　使用手引書 - UNIX/Windows(R)共通 -
・Systemwalker Operation Manager　リファレンスマニュアル - UNIX/Windows(R)共通 -
・Systemwalker Operation Manager　メッセージ説明書 - UNIX/Windows(R)共通 -
・Systemwalker Operation Manager　トラブルシューティングガイド - UNIX/Windows(R)共通 -
・Systemwalker Operation Manager スケジュール分散機能説明書 - UNIX/Windows(R)共通 -

【保証要件根拠】

保証手段に示した資料には、TOE の管理者が使用するインタフェース、TOE をセキュアに運用するための警告を含む使用方法、及び TOE の障害時に管理者が採るべきアクションについて規定する。そのため、保証要件 AGD_ADM.1 は満たされる。

AGD_USR.1　　利用者ガイダンス

【保証手段】

・Systemwalker Operation Manager セキュリティガイド
・Systemwalker Operation Manager　解説書 - UNIX/Windows(R)共通 -
・Systemwalker Operation Manager　導入手引書 - UNIX/Windows(R)共通 -
・Systemwalker Operation Manager　使用手引書 - UNIX/Windows(R)共通 -
・Systemwalker Operation Manager　リファレンスマニュアル - UNIX/Windows(R)共通 -
・Systemwalker Operation Manager　メッセージ説明書 - UNIX/Windows(R)共通 -
・Systemwalker Operation Manager　トラブルシューティングガイド - UNIX/Windows(R)共通 -

・Systemwalker Operation Manager スケジュール分散機能説明書 - UNIX/Windows(R)共通 -

【保証要件根拠】

保証手段に示した資料には、TOE の利用者が使用するインタフェース、及び TOE のセキュアな運用のための警告を含む使用方法を規定する。そのため、保証要件 AGD_USR.1 は満たされる。

ATE_IND.1　　独立テスト - 準拠

【保証手段】

TOE

【保証要件根拠】

テストに適した TOE を提供する。そのため、ATE_IND.1 は満たされる。

8.4 PP主張根拠

本 ST が参照する PP はない。

（　最終ページ　）